



Съвет на
Европейския съюз

Брюксел, 14 септември 2018 г.
(OR. en)

12104/18

Междуетноститутуционално досие:
2018/0328 (COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

ПРИДРУЖИТЕЛНО ПИСМО

От:	Генералния секретар на Европейската комисия, подписано от г-н Jordi AYET PUIGARNAU, директор
Дата на получаване:	12 септември 2018 г.
До:	Г-н Jeppe TRANHOLM-MIKKELSEN, генерален секретар на Съвета на Европейския съюз
№ док. Ком.:	COM(2018) 630 final
Относно:	Предложение за РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежа от национални координационни центрове

Приложено се изпраща на делегациите документ COM(2018) 630 final.

Приложение: COM(2018) 630 final



ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

**за създаване на Европейски център за промишлени, технологични и
изследователски експертни познания в областта на киберсигурността и Мрежа от
национални координационни центрове**

*Принос на Европейската комисия към срещата на лидерите в Залцбург на 19—20
септември 2018 г.*

{SEC(2018) 396 final} - {SWD(2018) 403 final} - {SWD(2018) 404 final}

Обяснителен меморандум

1. КОНТЕКСТ НА ПРЕДЛОЖЕНИЕТО

• Основания и цели на предложението

Тъй като ежедневието и икономиките ни стават все по-зависими от цифровите технологии, гражданите стават все по-уязвими от тежки киберинциденти. Бъдещата ни сигурност зависи от подобряването на способностите да защитим Съюза от киберзаплахи, тъй като както гражданската инфраструктура, така и военният капацитет разчитат на надеждни цифрови системи.

С цел да се отговори на нарастващите предизвикателства, Съюзът непрекъснато увеличава своите дейности в тази област, като се основава на стратегията за киберсигурност¹ от 2013 г. и заложените в нея цели и принципи, за да насърчи надеждна, безопасна и отворена кибернетична екосистема. През 2016 г. Съюзът прие своите първи мерки в областта на киберсигурността чрез Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета² относно сигурността на мрежите и информационните системи.

С оглед на бързо развиващата се ситуация в областта на киберсигурността, през септември 2017 г. Комисията и върховният представител на Съюза по въпросите на външните работи и политиката на сигурност представиха съвместното съобщение³ „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“ с цел да се укрепят допълнително устойчивостта, възпирането и реагирането срещу кибератаки на Съюза. В съвместното съобщение, основаващо се също така на предходни инициативи, е очертан набор от предложени действия, които включват, наред с друго, укрепване на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA), създаване на доброволна европейска рамка за сертифициране за киберсигурност, за да се повиши киберсигурността на продуктите и услугите в цифровия свят, както и план за бързо координирано реагиране при широкомащабни инциденти и кризи, свързани с киберсигурността.

В съвместното съобщение бе признато, че Съюзът също така има стратегически интерес да осигури запазването и развитието на ключовия технически потенциал, свързан с киберсигурността, за да защити своя цифров единен пазар, и по-специално да защити критичните мрежи и информационни системи и да предоставя основни услуги в сферата на киберсигурността. Съюзът трябва да бъде в състояние самостоятелно да осигурява своите цифрови активи и да се конкурира на световния пазар на решения, свързани с киберсигурността.

¹ СЪВМЕСТНО СЪОБЩЕНИЕ ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА „Стратегия на Европейския съюз за киберсигурност: отворено, безопасно и сигурно киберпространство“, JOIN/2013/01 final

² Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194, 19.7.2016 г., стр. 1).

³ СЪВМЕСТНО СЪОБЩЕНИЕ ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС, JOIN/2017/450 final.

В момента Съюзът е нетен вносител на свързани с киберсигурността продукти и решения и до голяма степен зависи от доставчици извън Европа⁴. Пазарът на решения, свързани с киберсигурността, е пазар на стойност 600 милиарда евро в световен мащаб, който се очаква да нарасне през следващите пет години средно с приблизително 17 % по отношение на продажбите, броя на дружествата и заетостта. Въпреки това, едва 6 от първите 20 държави, водещи в областта на киберсигурността от пазарна гледна точка, са държави членки⁵.

В същото време в Съюза съществува богат експертен и практически опит в областта на киберсигурността — повече от 660 организации от целия ЕС се регистрираха при картографирането на експертните центрове по въпросите на киберсигурността, проведено наскоро от Комисията⁶. Ако бъде преобразуван в продукти и услуги, които могат да се предлагат на пазара, този експертен опит би могъл да позволи на Съюза да обхване цялата верига за създаване на стойност, свързана с киберсигурността. Въпреки това усилията на научноизследователските и промишлените общности са разпокъсани, липсват им съгласуваност и обща мисия, което възпрепятства конкурентоспособността на ЕС в тази област, както и способността му да осигурява своите цифрови активи. Съответните сектори (например енергетика, космическа промишленост, отбрана, транспорт) и подобласти на киберсигурността днес получават недостатъчна подкрепа⁷. В Европа полезните взаимодействия между секторите на гражданската киберсигурност и киберсигурността, свързана с отбраната, също не са експлоатирани в пълна степен.

Създаването през 2016 г. на публично-частно партньорство (договорно публично-частно партньорство — ДПЧП) в областта на киберсигурността в Съюза беше солидна първа стъпка, която обедини общностите от научноизследователския, промишления и публичния сектор, за да се улеснят научните изследвания и иновациите в областта на киберсигурността, и която в границите на финансовата рамка за периода 2014 — 2020 г. следва да доведе до добри, по-целенасочени резултати в областта на научните изследвания и иновациите. Договорното публично-частно партньорство позволи на партньорите от промишления сектор да поемат задължения за индивидуалните разходи, които ще направят по областите, определени в стратегическата програма за научни изследвания и иновации на ДПЧП.

ЕС може обаче да се стреми към много по-мащабни инвестиции и се нуждае от по-ефективен механизъм, който би могъл да изгради траен капацитет, да обедини усилията и компетентностите и да стимулира разработването на новаторски решения, отговарящи на свързаните с киберсигурността предизвикателства в промишления сектор в областта на новите многоцелеви технологии (например изкуствен интелект, квантова изчислителна техника, блок-вериги и сигурна цифрова самоличност), както и в сектори от критично значение (например транспорт, енергетика, здравеопазване, финанси, държавно управление, далекосъобщения, производство, отбрана, космическа промишленост).

⁴ Проект на окончателен доклад относно проучването на пазара на решения, свързани с киберсигурността, 2018 г.

⁵ Проект на окончателен доклад относно проучването на пазара на решения, свързани с киберсигурността, 2018 г.

⁶ Технически доклади на Съвместния изследователски център: Европейски експертни центрове по въпросите на киберсигурността, 2018 г.

⁷ Технически доклад на Съвместния изследователски център: Резултати от картографирането (за подробности вж. приложения 4 и 5).

В съвместното съобщение е разгледана възможността за укрепване на способностите на Съюза за киберсигурност чрез мрежа от експертни центрове в сферата на киберсигурността, в чиято основа стои европейски експертен център в сферата на киберсигурността. Това ще има за цел да се допълнят съществуващите усилия за изграждане на потенциал в тази област на равнището на Съюза и на национално равнище. В съвместното съобщение беше изразено намерението на Комисията през 2018 г. да бъде предприета оценка на въздействието, за да се проучат съществуващите варианти с оглед създаването на структурата. Като първа стъпка и с цел получаване на информация за бъдещ размисъл, Комисията даде ход на пилотна фаза в рамките на програмата „Хоризонт 2020“, за да се помогне за обединяване на националните центрове в мрежа, така че да се даде нов тласък на развитието на компетентности и технологии в областта на киберсигурността.

На срещата на върха в областта на цифровите технологии в Талин през септември 2017 г. държавните и правителствените ръководители отправиха призив към Съюза да стане „световен лидер в областта на киберсигурността до 2025 г., за да се гарантират доверието, увереността и защитата на нашите граждани, потребители и предприемачи в мрежата и да се създаде възможност за свободен и законово регулиран интернет“.

В Заключенията на Съвета⁸, приети през ноември 2017 г., Комисията се призовава бързо да предостави оценка на въздействието относно възможните варианти и до средата на 2018 г. да предложи съответния правен инструмент за изпълнение на инициативата.

Програмата „Цифрова Европа“, предложена от Комисията през юни 2018 г.⁹, има за цел да разшири и максимално да увеличи ползите от цифровата трансформация за европейските граждани и предприятия във всички съответни области на политиката на ЕС, като укрепва политиките и подкрепя амбициите, свързани с цифровия единен пазар. Програмата предлага съгласуван и цялостен подход за гарантиране на най-успешното използване на модерните технологии, както и правилната комбинация от технически възможности и човешки компетентности за цифровата трансформация — не само в областта на киберсигурността, но също и по отношение на интелигентните инфраструктури за данни, изкуствения интелект, авангардните умения и приложения в промишлеността и в областите от обществен интерес. Тези елементи са взаимозависими, взаимно се подсилват и ако бъдат насърчавани едновременно, могат да достигнат необходимия мащаб, който да позволи създаването на процъфтяваща икономика, основана на данни¹⁰. Програмата „Хоризонт Европа“¹¹ — следващата рамкова програма на ЕС за научни изследвания и иновации, също поставя киберсигурността сред своите приоритети.

В този контекст с настоящия регламент се предлага да се създаде Европейски център за промишлени, технологични и изследователски експертни познания в областта на

⁸ Заключения на Съвета относно Съвместното съобщение до Европейския парламент и Съвета „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“, приети от Съвета по общи въпроси на 20 ноември 2017 г.

⁹ COM/2018/434 Предложение за Регламент на Европейския парламент и на Съвета за създаване на програмата „Цифрова Европа“ за периода 2021 — 2027 г

¹⁰ Вж. SWD(2018) 305.

¹¹ COM/2018/435 Предложение за Регламент на Европейския парламент и на Съвета за създаване на Рамковата програма за научни изследвания и иновации „Хоризонт Европа“ и за определяне на нейните правила за участие и разпространение на резултатите

киберсигурността с мрежа от национални координационни центрове. Този създаден за целта модел на сътрудничество следва да функционира както следва, за да стимулира европейската технологична и промишлена екосистема: Центърът за експертни познания ще улеснява и подпомага координирането на работата на мрежата и ще подпомага Експертната общност в сферата на киберсигурността, насочвайки развитието в областта на технологиите за киберсигурност и улеснявайки достъпа до събрания по този начин експертен опит. По-специално, центърът за експертни познания ще постига това чрез изпълнението на съответните части на програмите „Цифрова Европа“ и от „Хоризонт Европа“ чрез отпускане на безвъзмездни средства и извършване на обществени поръчки. С оглед на значителните инвестиции в киберсигурност, направени в други части на света, и на необходимостта от координиране и обединяване на съответните ресурси в Европа, Центърът за експертни познания се предлага като европейско партньорство¹², като по този начин се улесняват съвместните инвестиции от Съюза, държавите членки и/или промишлеността. Поради това предложението изисква държавите членки да допринасят в пропорционален размер за действията на Центъра за експертни познания и мрежата. Основният орган за вземане на решения е управителният съвет, в който участват всички държави членки, но само държавите членки, които участват финансово, имат право на глас. Механизмът на гласуване в управителния съвет следва принцип на двойно мнозинство, изискващ 75 % от финансовата вноска и 75 % от гласовете. Предвид отговорността, която носи за бюджета на Съюза, Комисията притежава 50 % от гласовете. Когато е уместно, за работата си в управителния съвет Комисията ще се възползва от експертния опит на Европейската служба за външна дейност. Управителният съвет се подпомага от Промислен и научен консултативен съвет, за да се гарантира редовен диалог с частния сектор, потребителски организации и други съответни заинтересовани страни.

В тясно сътрудничество с Мрежата от национални координационни центрове и експертната общност в сферата на киберсигурността (в които са ангажирани голяма група различни участници, занимаващи се с разработването на технологии за киберсигурност, като например научноизследователски организации, отраслите, свързани както с предлагането, така и с търсенето, и публичният сектор), създадени с настоящия регламент, Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността ще бъде основният изпълнителен орган за финансовите ресурси на ЕС, предназначени за киберсигурността по линия на предложените *програми „Цифрова Европа“ и „Хоризонт Европа“*.

Такъв всеобхватен подход би позволил да се подкрепи киберсигурността по цялата верига за създаване на стойност, от научните изследвания до подкрепата за внедряването и навлизането на ключови технологии. Финансовото участие на държавите членки следва да бъде съизмеримо с финансовата вноска на ЕС в настоящата инициатива и е крайно необходим елемент за нейния успех.

Предвид нейния конкретен опит и широкото и балансирано представителство на заинтересованите страни в нея, Европейската организация по киберсигурност, която е

¹² Както е определено в COM/2018/435 Предложение за Регламент на Европейския парламент и на Съвета за създаване на Рамковата програма за научни изследвания и иновации „Хоризонт Европа“ и за определяне на нейните правила за участие и разпространение на резултатите и както е посочено в COM/2018/434 final Предложение за Регламент на Европейския парламент и на Съвета за създаване на програмата „Цифрова Европа“ за периода 2021 — 2027 г.

съответният контрагент на Комисията в договорното публично-частно партньорство в областта на киберсигурността в рамките на „Хоризонт 2020“, следва да бъде поканена да участва в работата на Центъра и Мрежата.-.

В допълнение, Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността следва също така да се стреми да засили полезните взаимодействия между гражданското и свързаното с отбраната измерение на киберсигурността. Той следва да оказва подкрепа на държавите членки и на други заинтересовани участници, като предоставя консултации, споделя експертни познания и улеснява сътрудничеството във връзка с проектите и дейностите. При поискване от страна на държавите членки той може също така да изпълнява функцията на ръководител на проекти, особено по отношение на Европейския фонд за отбрана. Настоящата инициатива има за цел да допринесе за справяне със следните проблеми:

- **Недостатъчно сътрудничество между отраслите, свързани с предлагането и търсенето на киберсигурност.** Европейските предприятия са изправени пред предизвикателството да останат сигурни и едновременно с това да предлагат сигурни продукти и услуги на своите клиенти. Често обаче те не са в състояние по подходящ начин да гарантират сигурността на своите съществуващи продукти, услуги и активи или да разработят сигурни иновативни продукти и услуги. Основните активи за осигуряване на киберсигурност често са твърде скъпи, за да бъдат разработени и създадени от отделни участници, чиято основна стопанска дейност не е свързана с киберсигурността. В същото време връзките между търсенето и предлагането на пазара на решения, свързани с киберсигурността, не са достатъчно добре развити, което води до недостатъчно оптимално предлагане на европейски продукти и решения, адаптирани към потребностите на различните сектори, както и до недостатъчни равнища на доверие сред участниците на пазара.
- **Липса на ефикасен механизъм за сътрудничество между държавите членки за изграждане на потенциал в промишления сектор.** Понастоящем също така не съществува ефикасен механизъм за сътрудничество, чрез който държавите членки да могат да работят заедно за изграждане на необходимите възможности за подкрепа на иновациите в сферата на киберсигурността в различните промишлени сектори и за внедряване на авангардни европейски решения в областта на киберсигурността. Съществуващите механизми за сътрудничество за държавите членки в областта на киберсигурността съгласно Директива (ЕС) 2016/1148 не предвиждат такъв тип дейности в своя мандат.
- **Недостатъчно сътрудничество в рамките на и между научноизследователските и промишлените общности.** Въпреки теоретичния потенциал на Европа да обхване цялата верига за създаване на стойност, свързана с киберсигурността, съществуват съответни сектори (например енергетика, космическа промишленост, отбрана, транспорт) и подобласти на киберсигурността, които понастоящем получават слаба подкрепа от научноизследователската общност или са подкрепяни само от ограничен брой центрове (например постквантова и квантова криптография, удостоверяване и киберсигурност при изкуствения интелект). Въпреки че това сътрудничество очевидно съществува, то много често представлява краткосрочна договореност от типа на консултантско споразумение, която не дава възможност за участие в дългосрочни планове за научни изследвания за разрешаване на свързаните с киберсигурността предизвикателства в промишлеността.

- **Недостатъчно сътрудничество между общностите за научни изследвания и иновации в секторите на гражданската киберсигурност и киберсигурността, свързана с отбраната.** Проблемът с недостатъчните равнища на сътрудничество засяга и общностите в гражданския сектор и сектора, свързан с отбраната. Съществуващите полезни взаимодействия не се използват в пълна степен поради липсата на ефикасни механизми, позволяващи на тези общности да си сътрудничат ефикасно и да изграждат доверие, което е необходима предпоставка за успешно сътрудничество дори повече, отколкото в други области. Това е съчетано с ограничени финансови възможности на пазара на ЕС на решения, свързани с киберсигурността, включително недостатъчно средства за подкрепа на иновациите.
- **Съгласуваност със съществуващите разпоредби в тази област на политиката**

Мрежата за компетентност в сферата на киберсигурността и Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността ще действат като допълнителна подкрепа на съществуващите разпоредби и участници в областта на политиката за киберсигурността. Мандатът на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността ще допълва усилията на ENISA, но има различен фокус и изисква различен набор от умения. Докато мандатът на ENISA предвижда консултативна роля при научните изследвания и иновациите в областта на киберсигурността в ЕС, предложеният мандат на центъра се съсредоточава преди всичко върху други задачи, които са от съществено значение за укрепване на устойчивостта срещу киберзаплахи в ЕС. Освен това мандатът на ENISA не предвижда видовете дейности, които ще представляват основните задачи на Центъра и Мрежата — да се стимулират разработването и внедряването на технологии в областта на киберсигурността и да се допълнят усилията за изграждане на потенциал в тази област на равнище ЕС и на национално равнище.

Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността, заедно с Мрежата за компетентност в сферата на киберсигурността, ще работят и за подпомагане на научните изследвания с цел улесняване и ускоряване на процесите по стандартизация и сертифициране, и по-специално онези, свързани със схемите за сертифициране на киберсигурността по смисъла на предложението за Акт за киберсигурността^{13 14}.

С настоящата инициатива *de facto* се увеличава мащабът на публично-частното партньорство в областта на киберсигурността (ДПЧП), което е първият опит, обхващащ целия ЕС, за обединяване на сектора на киберсигурността, сектора на търсенето (купувачите на свързани с киберсигурността продукти и решения, включително публичната администрация и сектори от критично значение, като например транспорта,

¹³ Предложение за Регламент на Европейския парламент и на Съвета относно ENISA — Агенцията на ЕС за киберсигурност, и за отмяна на Регламент (ЕС) № 526/2013, както и относно сертифицирането на киберсигурността на информационните и комуникационните технологии („Акт за киберсигурността“, COM(2017) 477 final/3)

¹⁴ Това не засяга механизмите за сертифициране, предвидени в Общия регламент относно защитата на данните, в които органи по защита на данните имат определена роля, в съответствие с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

здравеопазването, енергетиката, финансите) и научноизследователската общност, за да се изгради платформа за устойчив диалог и да се създадат условия за доброволни съвместни инвестиции. Договорното публично-частно партньорство беше създадено през 2016 г. и до 2020 г. привлече инвестиции на стойност до 1,8 милиарда евро. Въпреки това мащабът на инвестициите, които понастоящем се реализират в други части на света (например само през 2017 г. САЩ инвестираха 19 милиарда долара в киберсигурност), показва, че ЕС трябва да положи повече усилия, за да постигне критична маса на инвестициите и да преодолее фрагментирането на капацитета, разпръснат в ЕС.

- **Съгласуваност с други политики на Съюза**

Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността ще играе ролята на единен изпълнителен орган за различните програми на Съюза за подпомагане на киберсигурността (програмите „Цифрова Европа“ и „Хоризонт Европа“) и ще засили съгласуваността и полезните взаимодействия между тях.

Настоящата инициатива ще позволи също така да се допълнят усилията на държавите членки, като се осигури подходящ принос за създателите на политики в областта на образованието, за да се подобрят уменията в сферата на киберсигурността (например като се разработят учебни програми по въпросите на киберсигурността в гражданската и военната образователна система), с цел да се подпомогне развитието на квалифицирана в областта на киберсигурността работна сила в ЕС — ключов актив за предприятията в сектора на киберсигурността, както и за други отрасли с интереси в областта на киберсигурността. Що се отнася до образованието и обучението в областта на киберотбраната, настоящата инициатива ще бъде в съответствие с текущата работа на платформата за образование, обучение и упражнения в областта на киберотбраната, създадена в рамките на Европейския колеж по сигурност и отбрана.

Настоящата инициатива ще допълва и подпомага усилията на цифровите иновационни центрове в рамките на програмата „Цифрова Европа“. Цифровите иновационни центрове са организации с нестопанска цел, които помагат на предприятията — особено на новосъздадените предприятия, МСП и дружествата със средна пазарна капитализация, да станат по-конкурентоспособни, като подобряват своите процеси на стопанска дейност/производство, както и своите продукти и услуги чрез интелигентни иновации, за които способстват цифровите технологии. Цифровите иновационни центрове предоставят ориентирани към бизнеса иновационни услуги, като например проучване на пазара, консултации за финансиране, достъп до подходящи изпитвателни и експериментални съоръжения, обучение и развитие на умения, за да помогнат за успешното достигане до пазара на нови продукти и услуги или за въвеждането на подобри производствени процеси. Някои цифрови иновационни центрове със специфични експертни познания в областта на киберсигурността биха могли директно да се включат в експертната общност в сферата на киберсигурността, създадена с настоящата инициатива. В повечето случаи обаче цифровите иновационни центрове, които нямат конкретен профил, свързан с киберсигурността, ще улесняват в своя район достъпа до експертен опит, познания и потенциал в областта на киберсигурността, с които разполага експертната общност в сферата на киберсигурността, като си сътрудничат тясно с Мрежата от национални координационни центрове и Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността. Цифровите иновационни центрове също така ще подпомагат

навлизането на иновативни свързани с киберсигурността продукти и решения, съответстващи на нуждите на предприятията и другите крайни ползватели, които обслужват. Не на последно място, специфичните за даден сектор цифрови иновационни центрове могат да споделят знанията си за реалните нужди на сектора с Мрежата и Центъра, за да информират анализа на програмата за научни изследвания и иновации в отговор на изискванията на промишления сектор.

Ще се търсят полезни взаимодействия със съответните общности на знание и иновации към Европейския институт за иновации и технологии (EIT), и по-специално с „EIT — Цифрови технологии“.

2. ПРАВНО ОСНОВАНИЕ, СУБСИДИАРНОСТ И ПРОПРОЦИОНАЛНОСТ

• Правно основание

Експертният център следва да бъде създаден въз основа на двойно правно основание поради неговия характер и специфичните му цели. Разпоредбата на член 187 отДФЕС, която предвижда създаването на структурите, необходими за ефективното осъществяване на програмите за научни изследвания, технологично развитие и демонстрационни дейности на Съюза, позволява на Експертния център да създава полезни взаимодействия и да обединява ресурси, за да инвестира в необходимия капацитет на равнище държави членки и да изгражда европейски общи активи (например чрез съвместни обществени поръчки за необходимите изпитвателни и експериментални инфраструктури в областта на киберсигурността). Член 188, параграф 1 предвижда приемането на такива мерки. Независимо от това, член 188, алинея първа като единствено правно основание не би позволил дейностите да надхвърлят сферата на научните изследвания и развитие, ако това е необходимо за изпълнението на всички предвидени в настоящия регламент цели на Експертния център за подпомагане на навлизането на пазара на свързани с киберсигурността продукти и решения, помощ за постигане на по-голяма конкурентоспособност на европейския сектор за киберсигурност и увеличаване на пазарния му дял, както и добавяне на стойност към националните усилия за преодоляване на недостига на умения в сферата на киберсигурността. Ето защо, за да бъдат постигнати тези цели, е необходимо като правно основание да се добави член 173, параграф 3, който позволява Съюзът да предвиди мерки в подкрепа на конкурентоспособността на сектора.

• Обосновка на предложението от гледна точка на принципите на субсидиарност и пропорционалност

Киберсигурността е въпрос от общ интерес за Съюза, както е потвърдено в Заключенията на Съвета, посочени по-горе. Мащабът и трансграничният характер на кибератаки като *WannaCry* или *NonPetya* са важно основание за това. Естеството и мащабът на технологичните предизвикателства пред киберсигурността, а също и недостатъчната координация на усилията в рамките на промишлеността, както и между промишления и публичния сектор и научноизследователските общности, налагат на ЕС допълнително да подкрепи усилията за координиране, както за да обедини критична маса от ресурси, така и за да осигури по-добри познания и управление на активите. Това е необходимо с оглед на изискванията относно ресурсите, свързани с определени възможности за изследване, разработване и внедряване на продукти и услуги за киберсигурност; необходимостта да се предостави достъп до интердисциплинарен експертен опит в сферата на киберсигурността между различните дисциплини (каквото често съществува само отчасти на национално равнище); глобалния характер на

промишлените вериги за създаване на стойност, както и дейността на конкурентите в световен мащаб, която те осъществяват на различните пазари.

Това изисква ресурси и експертни познания с мащаб, който трудно може да бъде постигнат чрез индивидуалните действия на която и да е държава членка. Така например, за общоевропейска мрежа за квантови комуникации може да са необходими инвестиции от ЕС на стойност приблизително 900 милиона евро, в зависимост от инвестициите от държавите членки (за свързване/допълване) и това до каква степен технологията ще позволи повторното използване на съществуващи инфраструктури. Инициативата ще способства за обединяването на финансови ресурси и създаването на условия за осъществяване на този вид инвестиции в Съюза.

Целите на настоящата инициатива не могат да бъдат постигнати в пълна степен със самостоятелните усилия на държавите членки. Както беше показано по-горе, те могат да бъдат постигнати по-добре на равнището на Съюза чрез обединяване на усилията и избягване на ненужното им дублиране, което ще помогне да се постигне критична маса на инвестициите и да се гарантира, че публичното финансиране се използва по най-оптимален начин. В същото време, в съответствие с принципа на пропорционалност настоящият регламент не надхвърля това, което е необходимо за постигането на тази цел. Следователно действията на равнище ЕС са оправдани от гледна точка на субсидиарността и пропорционалността.

Настоящият инструмент не предвижда нови законоустановени задължения за предприятията. В същото време предприятията, и по-специално МСП, вероятно ще намалят разходите, свързани с техните усилия за създаване на иновативни продукти, защитени срещу киберзаплахи, тъй като инициативата позволява да се обединят ресурси, за да бъдат инвестирани в необходимия капацитет на равнище държави членки или в изграждането на европейски общи активи (например чрез съвместни обществени поръчки за необходимите изпитвателни и експериментални инфраструктури в областта на киберсигурността). Тези активи могат да бъдат използвани от отрасли и МСП в различни сектори, за да се гарантира, че техните продукти са защитени срещу киберзаплахи и ще превърнат киберсигурността в тяхно конкурентно предимство.

- **Избор на инструмент**

С предложения инструмент се създава орган, предназначен да изпълнява действията в областта на киберсигурността по програма „Цифрова Европа“ и програма „Хоризонт Европа“. В инструмента са очертани мандатът, задачите, както и управленската структура на органа. За създаването на такъв орган на Съюза е необходимо приемането на регламент.

3. КОНСУЛТАЦИИ СЪС ЗАИНТЕРЕСОВАНИТЕ СТРАНИ И ОЦЕНКИ НА ВЪЗДЕЙСТВИЕТО

Предложението за създаване на Мрежа за компетентност в сферата на киберсигурността с Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността е нова инициатива. То изпълнява ролята на продължение на договорното публично-частно партньорство в областта на киберсигурността, създадено през 2016 г., и има за цел да увеличи мащаба му.

- **Консултации със заинтересованите страни**

Киберсигурността е широкообхватна, междусекторна тема. Комисията използва различни методи за консултации, за да се увери, че интересите на широката общественост в Съюза — а не специфичните интереси на тесен кръг от групи заинтересовани страни — са добре отразени в настоящата инициатива. Този метод гарантира прозрачност и отчетност в работата на Комисията. Въпреки че не беше проведена открита обществена консултация специално за настоящата инициатива, като се има предвид нейната целева аудитория (промишлената и научноизследователската общност и държавите членки), тематиката вече беше обхваната в няколко други открити обществени консултации:

- обща открита обществена консултация, проведена през 2018 г., по въпросите на инвестициите, научните изследвания и иновациите, малките и средните предприятия и единния пазар;
- 12-седмична обществена консултация онлайн, стартирана през 2017 г., за да се потърсят мненията на широката общественост (с приблизително 90 участници) относно оценката и прегледа на ENISA;
- 12-седмична обществена консултация онлайн, която беше проведена през 2016 г. по повод на стартирането на договорното публично-частно партньорство в областта на киберсигурността (с приблизително 240 участници).

Комисията също така организира целеви консултации относно настоящата инициатива, включително семинари, срещи и целеви искания за предоставяне на информация (от ENISA и Европейската агенция по отбрана). Периодът на консултацията надхвърли 6 месеца, като започна през ноември 2017 г. и продължи до март 2018 г. Комисията също така извърши картографиране на експертните центрове, което позволи събирането на информация от 665 експертни центрове по въпросите на киберсигурността относно техния експертен опит, дейности, области на работа и международно сътрудничество. На проучването беше даден ход през януари и за анализа на доклада бяха взети предвид проучванията, подадени до 8 март 2018 г.

Заинтересованите страни от промишлените и научноизследователските общности изразиха мнение, че Експертният център и Мрежата биха могли да добавят стойност към настоящите усилия на национално равнище, като спомогнат за създаването на екосистема на киберсигурността, обхващаща цяла Европа, която да позволи подобряване на сътрудничеството между научноизследователските и промишлените общности. Те считат също, че е необходимо ЕС и държавите членки да възприемат активна, дългосрочна и стратегическа перспектива към промишлената политика в областта на сигурността, която не се изчерпва единствено с научни изследвания и иновации. Заинтересованите страни изразиха нужда да получат достъп до ключови възможности, като изпитвателни и експериментални съоръжения, както и от по-голяма амбиция за преодоляване на недостига на умения в сферата на киберсигурността, например чрез широкомащабни европейски проекти, които да привличат най-добрите таланти. Също така всичко, описано по-горе, се счита за необходимо, за да може Съюзът да бъде признат в световен мащаб като лидер в областта на киберсигурността.

В рамките на консултацияните действия, предприети от миналия септември¹⁵, както и в специалните заключения на Съвета¹⁶, държавите членки приветстваха намерението за създаване на Мрежа за компетентност в сферата на киберсигурността, за да се стимулира разработването и внедряването на технологии за киберсигурност, като подчертаха необходимостта от приобщаване в нея на всички държави членки и техните съществуващи експертни центрове и центрове за компетентност, както и от това да се обърне специално внимание на взаимното допълване. Конкретно във връзка с бъдещия Експертен център държавите членки подчертаха значението на неговата координираща роля при подпомагането на мрежата. По-специално по отношение на националните дейности и нужди в областта на киберотбраната, картографирането на нуждите на държавите членки в областта на киберотбраната, проведено от Европейската служба за външна дейност през март 2018 г., показва, че повечето държави членки виждат добавена стойност в подкрепата от ЕС при обучението и образованието в областта на киберотбраната, както и в подкрепата на промишлеността чрез научноизследователска и развойна дейност¹⁷. Инициативата на практика ще се изпълнява заедно с държавите членки или образуванията, подкрепяни от тях. Сътрудничеството между общностите от промишления, научноизследователския и публичния сектор би обединило и укрепило съществуващите образувания и усилия, вместо да създава нови. Държавите членки ще участват също така в определянето на конкретни действия, насочени към публичния сектор като пряк ползвател на технологиите и експертния опит за киберсигурност.

- **Оценка на въздействието**

На 11 април 2017 г. на Комитета за регулаторен контрол беше представена оценка на въздействието в подкрепа на настоящата инициатива и по нея беше дадено положително становище с резерви. Оценката на въздействието впоследствие беше преразгледана в светлината на коментарите на комитета. Становището на комитета и приложението, в което се обяснява какви мерки са взети по коментарите на комитета, са публикувани заедно с настоящото предложение.

В оценката на въздействието бяха разгледани редица варианти на политиката, както законодателни, така и незаконодателни. Следните варианти бяха запазени за задълбочена оценка:

- базовият сценарий — вариант въз основа на сътрудничество — предполага продължаване на настоящия подход за изграждане на промишлен и технологичен потенциал в сферата на киберсигурността в ЕС чрез подкрепа на научните изследвания и иновациите и свързаните с тях механизми за сътрудничество в рамките на РП9;
- вариант 1: Мрежа за компетентност в сферата на киберсигурността с Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността с двустранен мандат за изпълнение на мерки в подкрепа на промишлените технологии, както и в сферата на научните изследвания и иновациите;

¹⁵ Напр. кръгла маса на високо равнище с държавите членки, заместник-председател Ансип, член на Комисията Габриел, 5 декември 2017 г.

¹⁶ Съвет по общи въпроси: Заключения на Съвета относно Съвместното съобщение до Европейския парламент и Съвета „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“ (20 ноември 2017 г.)

¹⁷ ЕСВД, март 2018 г.

- вариант 2: Мрежа за компетентност в сферата на киберсигурността с Европейски експертен център за научни изследвания в областта на киберсигурността, съсредоточени върху дейностите за научни изследвания и иновации.

Вариантите, отхвърлени на ранен етап, включваха: 1) варианта да не се предприемат действия, 2) варианта да се създаде само Мрежа за компетентност в сферата на киберсигурността, 3) варианта да се създаде само централизирана структура, както и 4) варианта да се използва съществуваща агенция (Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA), Изпълнителната агенция за научни изследвания (REA) или Изпълнителната агенция за иновации и мрежи (INEA).

В анализа се заключава, че вариант 1 е най-уместен за постигане на целите на инициативата, като същевременно предлага най-голямо икономическо, социално и екологично въздействие и защитава интересите на Съюза. Основните аргументи в полза на този вариант включват възможността за създаване на истинска промишлена политика в областта на киберсигурността чрез подкрепа на дейности, свързани не само с научноизследователска и развойна дейност, но и с навлизането на пазара; гъвкавостта, позволяваща различни модели на сътрудничество с мрежата от експертни центрове, за да се оптимизира използването на съществуващите знания и ресурси; способността за структуриране на сътрудничеството и съвместните ангажименти на заинтересованите страни от публичния и частния сектор, идващи от всички съответни сектори, включително сектора на отбраната; и не на последно място, вариант 1 позволява също така увеличаване на полезните взаимодействия и може да играе ролята на механизъм за изпълнение за двата различни потока на финансиране от ЕС в областта на киберсигурността по линия на следващата многогодишна финансова рамка (програмите „Цифрова Европа“ и „Хоризонт Европа“).

• Основни права

Настоящата инициатива ще позволи на публичните органи и отраслите във всички държави членки по-ефективно да предотвратяват и реагират на киберзаплахи, като предлагат и се обезпечават с по-сигурни продукти и решения. Това е от значение по-специално за защитата на достъпа до основни услуги (например транспорт, здравеопазване, банкови и финансови услуги).

Повишеният потенциал на Европейския съюз самостоятелно да осигурява своите продукти и услуги също вероятно ще помогне на гражданите да се ползват от своите демократични права и ценности (например по-добра защита на техните права, свързани с информацията, залегнали в Хартата на основните права, по-специално правото на защита на личните данни и правото на зачитане на личния живот) и следователно ще увеличи доверието им в цифровото общество и цифровата икономика.

4. ОТРАЖЕНИЕ ВЪРХУ БЮДЖЕТА

Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността, в сътрудничество с Мрежата за компетентност в сферата на киберсигурността, ще бъде основният изпълнителен орган за финансовите ресурси на ЕС, предназначени за киберсигурността, в рамките на програмите „Цифрова Европа“ и „Хоризонт Европа“.

Отражението върху бюджета, свързано с изпълнението на програмата „Цифрова Европа“, е описано подробно в законодателната финансова обосновка, приложена към

настоящото предложение. Финансовата вноска от финансовия пакет на клъстера „Приобщаващо и сигурно общество“ по стълб II „Глобални предизвикателства и конкурентоспособност на промишлеността“ в рамките на програма „Хоризонт Европа“ (общ пакет на стойност 2 800 000 000 евро), посочена в член 21, параграф 1, буква б), ще бъде предложена от Комисията по време на законодателния процес и във всеки случай преди да бъде постигнато политическо споразумение. Предложението ще се основава на резултатите от процеса на стратегическо планиране, както е определено в член 6, параграф 6 от Регламент XXX [рамкова програма „Хоризонт Европа“].

5. ДРУГИ ЕЛЕМЕНТИ

• Планове за изпълнение и механизъм за мониторинг, оценка и докладване

В настоящото предложение се предвижда изрична клауза за оценка (член 38), въз основа на която Комисията ще извършва независима оценка. Впоследствие Комисията ще докладва на Европейския парламент и на Съвета за своята оценка, която при необходимост ще бъде придружена от предложение за преразглеждане, за да се оценят въздействието на инструмента и неговата добавена стойност. При оценката ще бъде приложена методиката на Комисията за по-добро законотворчество.

Изпълнителният директор следва на всеки две години да представя на управителния съвет последваща оценка на дейността на Европейския център за промишлени, технологични и изследователски експертни познания и Мрежата, както е предвидено в член 17 от настоящото предложение. Изпълнителният директор следва също така на всеки две години да изготвя план за последващи действия във връзка със заключенията от предишни оценки и доклад за напредъка до Комисията. Управителният съвет следва да бъде отговорен за наблюдението на подходящи последващи действия по тези заключения, както е предвидено в член 16 от настоящото предложение.

Сигналите за случаи на лошо администриране на дейността от страна на юридическото лице може да бъдат предмет на разследване от страна на Европейския омбудсман в съответствие с разпоредбите на член 228 от Договора.

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА**за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежа от национални координационни центрове**

Принос на Европейската комисия към срещата на лидерите в Залцбург на 19—20 септември 2018 г.

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално член 173, параграф 3 и член 188, първа алинея от него,

като взеха предвид предложението на Европейската комисия,

като взеха предвид становището на Европейския икономически и социален комитет¹⁸,

като взеха предвид становището на Комитета на регионите¹⁹,

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

- (1) Ежедневието и икономиките ни стават все по-зависими от цифровите технологии, а с това гражданите стават все по-уязвими от тежки киберинциденти. Бъдещата ни сигурност зависи, наред с друго, от подобряването на технологичните и промишлените способности да защитим Съюза от киберзаплахи, тъй като както гражданската инфраструктура, така и военният капацитет разчитат на надеждни цифрови системи.
- (2) ЕС непрекъснато увеличава своите дейности за справяне с нарастващите предизвикателства, свързани с киберсигурността, като следва Стратегията за киберсигурност от 2013 г.²⁰, насочена към насърчаване на надеждна, безопасна и отворена кибернетична екосистема. През 2016 г. Съюзът прие първите мерки в областта на киберсигурността чрез Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета²¹ относно сигурността на мрежите и информационните системи.

¹⁸ ОВ С [...], [...] г., стр. [...].

¹⁹ ОВ С [...], [...] г., стр. [...].

²⁰ Съвместно съобщение до Европейския парламент и Съвета „Стратегия на Европейския съюз за киберсигурност: отворено, безопасно и сигурно киберпространство“, JOIN/2013/01 final.

²¹ Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194, 19.7.2016 г., стр. 1).

- (3) През септември 2017 г. Комисията и върховният представител на Съюза по въпросите на външните работи и политиката на сигурност представиха съвместното съобщение²² „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“ с цел да се укрепят допълнително устойчивостта, възпирането и реагирането срещу кибератаки на Съюза.
- (4) На срещата на върха в областта на цифровите технологии в Талин през септември 2017 г. държавните и правителствените ръководители отправиха призив към Съюза да стане „световен лидер в областта на киберсигурността до 2025 г., за да се гарантират доверието, увереността и защитата на нашите граждани, потребители и предприемачи в мрежата и да се създаде възможност за свободен и законово регулиран интернет“.
- (5) Значително смущение във функционирането на мрежите и информационните системи може да засегне отделните държави членки и Съюза като цяло. Ето защо сигурността на мрежите и информационните системи е от основно значение за безпрепятственото функциониране на вътрешния пазар. В момента Съюзът зависи от доставчици на киберсигурност извън Европа. Съюзът обаче има стратегически интерес да осигури запазването и развитието на ключовия технически потенциал, свързан с киберсигурността, за да защити своя цифров единен пазар, и по-специално да защити мрежите и информационните системи от критично значение и да предоставя основни услуги в сферата на киберсигурността.
- (6) В Съюза съществува богат експертен и практически опит в научните изследвания, технологиите и промишлените разработки в областта на киберсигурността, но усилията на промишлените и научноизследователските общности са разпокъсани, липсват им съгласуваност и обща мисия, което възпрепятства конкурентоспособността в тази област. Тези усилия и експертен опит трябва да бъдат обединени и да се изградят съответните контакти, така че те да бъдат използвани по ефикасен начин, за да се подсили и допълни съществуващият научноизследователски, технологичен и промишлен потенциал на равнището на Съюза и на национално равнище.
- (7) В Заключенията на Съвета, приети през ноември 2017 г., Комисията се призовава бързо да предостави оценка на въздействието относно възможните варианти за създаване на мрежа от центрове за компетентност в сферата на киберсигурността и Европейски експертен център за научни изследвания и до средата на 2018 г. да предложи съответния правен инструмент.
- (8) Експертният център, заедно с Мрежата за компетентност в сферата на киберсигурността, следва да бъде основният инструмент на Съюза за обединяване на инвестициите в научни изследвания, технологии и промишлени разработки в областта на киберсигурността и за изпълнение на съответните проекти и инициативи. Той следва да предоставя финансова подкрепа, свързана с киберсигурността, от програмите „Хоризонт Европа“ и „Цифрова Европа“ и когато е уместно до него следва да имат достъп Европейският фонд за регионално развитие и други програми. Този подход следва да допринесе за създаването на полезни взаимодействия и координирането на финансовата подкрепа, свързана с научните изследвания, иновациите, технологиите и

²²

Съвместно съобщение до Европейския парламент и Съвета „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“, JOIN/2017/450 final.

промишлените разработки в областта на киберсигурността, както и за избягване на дублирането.

- (9) Като се има предвид, че целите на настоящата инициатива могат да бъдат постигнати най-добре, ако участват всички или възможно най-много държави членки, като стимул за участие на държавите членки права на глас следва да получават само онези от тях, които допринасят финансово за покриване на административните и оперативните разходи на Експертния център.
- (10) Финансовото участие на участващите държави членки следва да бъде съизмеримо с финансовата вноска на Съюза по настоящата инициатива.
- (11) Експертният център следва да улеснява и да спомага за координиране на работата на Мрежата за компетентност в сферата на киберсигурността („Мрежата“), съставена от националните координационни центрове във всяка държава членка. Националните координационни центрове следва да получават директно финансово подпомагане от Съюза, включително отпускане на безвъзмездни средства без покана за представяне на предложения, за да извършват дейности по смисъла на настоящия регламент.
- (12) Националните координационни центрове следва да се избират от държавите членки. В допълнение към необходимия административен капацитет, центровете следва да притежават или да имат пряк достъп до технологичен опит в сферата на киберсигурността, по-специално в области като криптография, услуги за сигурност на ИКТ, откриване на проникване, сигурност на системите, сигурност на мрежите, сигурност на софтуера и приложенията или аспектите на сигурността и неприкосновеността на личния живот, свързани с обществото и личността. Те също така следва да имат капацитет ефективно да привличат и да се координират с промишления сектор, публичния сектор, включително органи, определени съгласно Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета²³ и научноизследователската общност,
- (13) Когато на националните координационни центрове се предоставя финансова подкрепа, за да подпомагат трети страни на национално равнище, тя се прехвърля на съответните заинтересовани страни чрез споразумения за отпускане на безвъзмездни средства на каскаден принцип.
- (14) Едновременно с предлагането на решения, нововъзникващите технологии, като изкуствен интелект, интернет на вещите, високопроизводителни изчислителни технологии и квантова изчислителна техника, блок-вериги и концепции като сигурна цифрова самоличност създават и нови предизвикателства за киберсигурността. За целите на оценката и валидирането на устойчивостта на съществуващите или бъдещите системи на ИКТ ще е нужно да се проведат изпитвания на решенията за сигурност срещу атаки, които се извършват на високопроизводителни изчислителни машини и квантови компютри. Експертният център, Мрежата и експертната общност в сферата на киберсигурността следва да помагат за развитието и разпространението на най-новите решения, свързани с киберсигурността. В същото време Експертният център и Мрежата следва да бъдат в услуга на разработчиците и операторите в

²³ Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194, 19.7.2016 г., стр. 1).

сектори от критично значение, като например транспорт, енергетика, здравеопазване, финанси, държавно управление, далекосъобщения, производство, отбрана и космическа промишленост, за да им помагат да се справят с предизвикателствата, свързани с киберсигурността, пред всеки от тях.

- (15) Експертният център следва да има няколко ключови функции. На първо място, експертният център следва да улеснява и да подпомага координирането на работата на Европейската мрежа за компетентност в сферата на киберсигурността и да развива експертната общност в сферата на киберсигурността. Центърът следва да бъде двигател на развитието в областта на технологиите за киберсигурност и да улесни достъпа до експертния опит, натрупан в Мрежата и експертната общност в сферата на киберсигурността. На второ място, той следва да изпълнява съответните части на програмите „Цифрова Европа“ и „Хоризонт Европа“, като разпределя безвъзмездни средства, обикновено вследствие на конкурсната покана за представяне на предложения. На трето място, Експертният център следва да улеснява съвместните инвестиции на Съюза, държавите членки и/или промишлеността.
- (16) Експертният център следва да стимулира и подкрепя сътрудничеството и координирането на дейностите на експертната общност в сферата на киберсигурността, в които ще са ангажирани голяма група различни участници, занимаващи се с технологии в областта на киберсигурността. Тази общност следва да обхваща по-специално научноизследователски организации, отраслите, свързани както с предлагането, така и с търсенето, и публичния сектор. Експертната общност в сферата на киберсигурността следва да предоставя принос към дейностите и работния план на експертния център и също така следва да се ползва от дейностите на Експертния център и Мрежата по изграждане на общността, но не трябва да бъде привилегирована по друг начин по отношение на поканите за представяне на предложения или поканите за участие в търг.
- (17) За да се отговори на нуждите на отраслите, свързани както с търсенето, така и с предлагането, задачата на Експертния център да предоставя знания и техническа помощ в областта на киберсигурността на отраслите следва да се отнася едновременно за продукти и услуги на ИКТ и за всички други промишлени и технологични продукти и решения, в които трябва да бъде вграден елемент на киберсигурност.
- (18) Като се има предвид, че Експертният център и Мрежата следва да се стремят да постигнат полезни взаимодействия между гражданската и свързаната с отбраната сфера на киберсигурността, проектите, финансирани по програма „Хоризонт Европа“, ще се изпълняват в съответствие с Регламент XXX [Регламента за „Хоризонт Европа“], който предвижда провежданите дейности по научни изследвания и иновации по линия на „Хоризонт Европа“ да бъдат съсредоточени върху приложения за граждански цели.
- (19) За да се осигури структурирано и устойчиво сътрудничество, отношенията между Експертния център и националните координационни центрове следва да се основават на договорно споразумение.
- (20) Следва да се предвидят подходящи разпоредби за гарантиране на отговорността и прозрачността на Експертния център.

- (21) С оглед на техния съответен експертен опит в областта на киберсигурността Съвместният изследователски център на Комисията, както и Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) следва да имат активна роля в експертната общност в сферата на киберсигурността и в Промисления и научен консултативен съвет.
- (22) Когато националните координационни центрове и образуванията, които са част от експертната общност в сферата на киберсигурността, получават финансови вноски от общия бюджет на Съюза, те следва да оповестяват публично факта, че съответните дейности се осъществяват в контекста на настоящата инициатива.
- (23) С финансовата вноска на Съюза за Експертния център следва да се финансират половината от разходите за създаването и административните и координационните дейности на Експертния център. С цел да се избегне двойно финансиране, тези дейности не трябва да получават едновременно финансова вноска от други програми на Съюза.
- (24) Управителният съвет на Експертния център, състоящ се от държавите членки и Комисията, следва да определя общата насока на дейността на Експертния център и да гарантира, че той изпълнява своите задачи в съответствие с настоящия регламент. Управителният съвет следва да получи правомощията, необходими за определяне на бюджета, проверка на неговото изпълнение, приемане на подходящи финансови правила, установяване на прозрачни работни процедури за вземане на решения от страна на Експертния център, приемане на работния план и многогодишния стратегически план на Експертния център с оглед на приоритетите за постигане на целите и задачите му, приемане на собствен правилник за дейността на центъра, назначаване на изпълнителния директор и вземане на решения за удължаване или прекратяване на неговия мандат.
- (25) С оглед на правилното и ефективно функциониране на Експертния център Комисията и държавите членки следва да гарантират, че лицата, назначени в управителния съвет, притежават подходяща професионална компетентност, както и опит в областите на работа. Комисията и държавите членки следва също да положат усилия да намалят текучеството на своите съответни представители в управителния съвет, за да се гарантира непрекъснатост на работата му.
- (26) Безпрепятственото функциониране на Експертния център налага неговият изпълнителен директор да се назначава въз основа на неговите заслуги и документиран административни и управленски умения, както и въз основа на неговите компетентност и опит, свързани с киберсигурността, като той трябва да изпълнява задълженията си в условия на пълна независимост.
- (27) Експертният център следва да разполага с Промислен и научен консултативен съвет в ролята на консултативен орган, за да се гарантира редовен диалог с частния сектор, потребителските организации и други подходящи заинтересовани страни. Промисленият и научен консултативен съвет следва да се съсредоточава върху въпроси, засягащи заинтересованите страни, и да насочва към тях вниманието на управителния съвет на Експертния център. Съставът на Промисления и научен консултативен съвет, както и възложените му задачи, като например консултиране във връзка с работния план, следва да гарантират достатъчна степен на представяне на заинтересованите страни в работата на Експертния център.

- (28) Експертният център следва да се ползва от специфичния експертен опит и широкото и балансирано представителство на заинтересованите страни, изградени чрез договорното публично-частно партньорство в областта на киберсигурността по време на периода на изпълнение на програмата „Хоризонт 2020“, чрез своя Промислен и научен консултативен съвет.
- (29) Експертният център следва да има правила за предотвратяването и управлението на конфликти на интереси. Експертният център следва също така да прилага съответните разпоредби на Съюза относно публичния достъп до документи, както е посочено в Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета²⁴. При обработката на лични данни от Експертния център се прилагат разпоредбите на Регламент (ЕС) № XXX/2018 на Европейския парламент и на Съвета. Експертният център следва да съблюдава разпоредбите, приложими за институциите на Съюза, както и националното законодателство относно обработката на информация, по-специално на чувствителната неклафицирана информация и на класифицирана информация на ЕС.
- (30) Финансовите интереси на Съюза и на държавите членки следва да бъдат защитени чрез прилагане на пропорционални мерки през целия цикъл на разходи, включително мерки за предотвратяване, разкриване и разследване на нередности, възстановяване на загубени, недължимо платени или неправилно използвани средства и, по целесъобразност, налагане на административни и финансови санкции в съответствие с Регламент (ЕС, Евратом) № XXX на Европейския парламент и на Съвета²⁵ [„Финансовия регламент“].
- (31) Експертният център следва да работи открито и прозрачно, като предоставя цялата съответна информация своевременно и популяризира дейностите си, включително по предоставяне и разпространяване на информация сред широката общественост. Правилникът за дейността на органите на Експертния център следва да бъде обществено достъпен.
- (32) Вътрешният одитор на Комисията следва да упражнява същите правомощия по отношение на Експертния център, каквито упражнява по отношение на Комисията.
- (33) Комисията, Експертният център, Сметната палата и Европейската служба за борба с измамите следва да получават достъп до цялата необходима информация и до помещенията, за да провеждат одити и разследвания на безвъзмездните средства, договорите и споразуменията, подписвани от Експертния център.
- (34) Тъй като целите на настоящия регламент, а именно запазването и развитието на технологичния и промишления потенциал на Съюза, свързан с киберсигурността, увеличаването на конкурентоспособността на сектора на киберсигурността на Съюза и превръщането на киберсигурността в конкурентно предимство на други отрасли на Съюза, не могат да бъдат постигнати в достатъчна степен от държавите членки поради факта, че ограничените налични ресурси са разпръснати, както и поради мащаба на необходимите инвестиции, но — от съображения да се избегне ненужното дублиране на тези усилия, да се

²⁴ Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета от 30 май 2001 г. относно публичния достъп до документи на Европейския парламент, на Съвета и на Комисията (ОВ L 145, 31.5.2001 г., стр. 43).

²⁵ [Да се добавят заглавието и номерът в Официален вестник]

помогне за постигане на критична маса на инвестициите и да се гарантира, че публичното финансиране се използва по най-оптимален начин, могат да бъдат постигнати по-добре на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от Договора за Европейския съюз. В съответствие с принципа на пропорционалност, уреден в същия член, настоящият регламент не надхвърля необходимото за постигането на тази цел,

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА 1

ОБЩИ РАЗПОРЕДБИ И ПРИНЦИПИ НА ЕКСПЕРТНИЯ ЦЕНТЪР И МРЕЖАТА

Член 1

Предмет

1. С настоящия регламент се създават Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността („Експертен център“), както и Мрежа от национални координационни центрове, и се определят правилата за издигане на кандидатури за национални координационни центрове, както и за създаването на експертната общност в сферата на киберсигурността.
2. Експертният център допринася за изпълнението на свързаната с киберсигурността част от програмата „Цифрова Европа“, създадена с Регламент № XXX, и по-специално дейностите от нея, свързани с член 6 от Регламент (ЕС) № XXX [програмата „Цифрова Европа“], и от програмата „Хоризонт Европа“, създадена с Регламент № XXX, и по-специално приложение I, стълб II, раздел 2.2.6 към Решение № XXX за създаване на специфичната програма за изпълнение на „Хоризонт Европа“ — рамковата програма за научни изследвания и иновации [спр. номер на конкретната програма].
3. Седалището на експертния център се намира в [Брюксел, Белгия].
4. Експертният център има юридическа правосубектност. Във всяка от държавите членки той притежава най-широката юридическа правоспособност, която се предоставя на юридическите лица съгласно законите на тази държава членка. Той може, по-специално, да придобива и да се разпорежда с движимо и недвижимо имущество и може да бъде страна в съдебни производства.

Член 2

Определения

За целите на настоящия регламент се прилагат следните определения:

- 1) „киберсигурност“ означава защитата от киберзаплахи на мрежите и информационните системи, на техните ползватели и други лица;

- 2) „свързани с киберсигурността продукти и решения“ означава продукти, услуги или процеси на ИКТ, чиято специфична цел е да защитават от киберзаплахи мрежите и информационните системи, техните ползватели и засегнатите лица;
- 3) „публичен орган“ означава всяка държавна или друга публична администрация, включително публични консултативни органи, на национално, регионално или местно равнище или всяко физическо или юридическо лице, което изпълнява публични административни функции съгласно националното законодателство, включително специфични задължения;
- 4) „участваща държава членка“ означава държава членка, която доброволно допринася финансово за покриване на административните и оперативните разходи на Експертния център.

Член 3

Мисия на Центъра и Мрежата

1. Експертният център и Мрежата помагат на Съюза:
 - а) да запазва и развива необходимия технически и промишлен потенциал, свързан с киберсигурността, за да защити своя цифров единен пазар;
 - б) да увеличава конкурентоспособността на своя отрасъл на киберсигурността и да превърне киберсигурността в конкурентно предимство на други свои отрасли.
2. Когато е уместно, Експертният център осъществява своите задачи в сътрудничество с Мрежата от национални координационни центрове и експертната общност в сферата на киберсигурността.

Член 4

Цели и задачи на центъра

Експертният център има следните цели и свързани с тях задачи:

1. да улеснява и да подпомага координирането на работата на Мрежата от национални координационни центрове („Мрежата“), посочена в член 6, и експертната общност в сферата на киберсигурността, посочена в член 8;
2. да допринася за изпълнението на свързаната с киберсигурността част от програмата „Цифрова Европа“, създадена с Регламент № XXX²⁶, и по-специално дейностите, свързани с член 6 от Регламент (ЕС) № XXX [програмата „Цифрова Европа“], и от програмата „Хоризонт Европа“, създадена с Регламент № XXX²⁷, и по-специално приложение I, стълб II, раздел 2.2.6 към Решение № XXX за създаване на специфичната програма за изпълнение на „Хоризонт Европа“ — рамковата програма за научни изследвания и иновации [спр. номер на конкретната програма] и други програми на Съюза, когато това е предвидено в правните актове на Съюза];

²⁶ [Да се добавят пълното заглавие и номерът в Официален вестник]

²⁷ [Да се добавят пълното заглавие и номерът в Официален вестник]

3. да подобрява капацитета, знанията и инфраструктурата, свързани с киберсигурността, в услуга на отраслите и публичния сектор и научноизследователските общности, като осъществява следните задачи:
- а) като взема предвид най-съвременните промишлени и научноизследователски инфраструктури в областта на киберсигурността и свързаните с тях услуги, да придобива, модернизира, експлоатира и предоставя такива инфраструктури и свързаните с тях услуги на широк кръг ползватели в целия Съюз, от промишления сектор, включително МСП, до публичния сектор и изследователската и научната общност,
 - б) като взема предвид най-съвременните промишлени и научноизследователски инфраструктури в областта на киберсигурността и свързаните с тях услуги, да предоставя подкрепа на други образувания, включително финансова, за придобиване, модернизиране, експлоатация и предоставяне на такива инфраструктури и свързаните с тях услуги на широк кръг ползватели в целия Съюз, от промишлеността, включително МСП, до публичния сектор и изследователската и научната общност,
 - в) да предоставя знания и техническа помощ във връзка с киберсигурността на промишлеността и публичните органи, по-специално чрез подкрепа на действия, целящи да улеснят достъпа до наличния опит в Мрежата и експертната общност в сферата на киберсигурността;
4. да допринася за широкото разпространение на най-съвременните продукти и решения за киберсигурност в цялата икономика, като изпълнява следните задачи:
- а) да стимулира научните изследвания и разработки в областта на киберсигурността и навлизането на свързани с киберсигурността продукти и решения на Съюза сред публичните органи и в отраслите на ползвателите,
 - б) да оказва съдействие на публичните органи, отраслите от страната на търсенето и другите ползватели при приемането и интегрирането на най-новите решения за киберсигурност,
 - в) да оказва особена подкрепа на публичните органи при организирането на техните обществени поръчки или да провежда процедури за обществени поръчки за най-съвременни свързани с киберсигурността продукти и решения от името на публичните органи,
 - г) да предоставя финансова подкрепа и техническа помощ на новосъздадените предприятия и МСП в сферата на киберсигурността за осъществяване на връзка с потенциални пазари и привличане на инвестиции;
5. да подобрява разбирането за киберсигурността и да допринася за намаляване недостига на умения в сферата на киберсигурността в Съюза, като изпълнява следните задачи:

- а) да подкрепя по-нататъшно развитие на уменията в сферата на киберсигурността, когато е уместно, заедно със съответните агенции и органи на ЕС, включително ENISA;
- 6. да допринася за укрепване на научните изследвания и развитието в сферата на киберсигурността в Съюза чрез:
 - а) предоставяне на финансова подкрепа за научноизследователската дейност в областта на киберсигурността въз основа на обща многогодишна стратегическа, промишлена, технологична и научноизследователска програма, подлежаща на постоянни оценки и подобрения,
 - б) подкрепа за широкомащабни изследователски и демонстрационни проекти за технологичен капацитет от следващо поколение, свързан с киберсигурността, в сътрудничество с отрасъла и Мрежата,
 - в) подкрепа на научните изследвания и иновациите, насочени към процесите по стандартизация в областта на технологиите за киберсигурност;
- 7. да подобрява сътрудничеството между гражданския сектор и сектора, свързан с отбраната, по отношение на технологиите и приложенията с двойна употреба в областта на киберсигурността, като изпълнява следните задачи:
 - а) да подпомага държавите членки и заинтересованите страни от промишления сектор и научната общност по отношение на научните изследвания, разработването и внедряването,
 - б) да допринася за сътрудничеството между държавите членки, като подкрепя образованието, обучението и практическите занимания,
 - в) обединявайки заинтересованите страни, да насърчава полезните взаимодействия между гражданския сектор и сектора на отбраната по отношение на научните изследвания и пазарите на продукти и услуги за киберсигурност;
- 8. да засили полезните взаимодействия между гражданското и свързаното с отбраната измерение на киберсигурността във връзка с Европейския фонд за отбрана, като изпълнява следните задачи:
 - а) да предоставя консултации, да споделя експертен опит и да улеснява сътрудничеството между съответните заинтересовани страни,
 - б) да управлява многонационални проекти в областта на киберотбраната по искане на държавите членки и по този начин да изпълнява функцията на ръководител на проекти по смисъла на Регламент XXX [Регламента за създаване на Европейския фонд за отбрана].

Член 5

Инвестиции във и използване на инфраструктури, капацитет, продукти или решения

1. Когато Експертният център предоставя финансиране за инфраструктури, капацитет, продукти или решения в съответствие с член 4, параграфи 3 и 4 под

формата на безвъзмездни средства или награда, в работния план на Експертния център може да бъдат определени, по-специално:

- а) правила, уреждащи експлоатацията на инфраструктурата или капацитета, включително, когато е уместно, възлагането на експлоатацията на образование — доставчик на хостинг, въз основа на критерии, които се определят от Експертния център,
 - б) правила, уреждащи достъпа до и използването на инфраструктурата или капацитета.
2. Експертният център може да отговаря за цялостното изпълнение на съответните съвместни процедури за възлагане на обществени поръчки, включително обществени поръчки за продукти в предпазарен стадий, от името на членовете на Мрежата, членовете на експертната общност в сферата на киберсигурността или други трети страни, представляващи ползвателите на свързани с киберсигурността продукти и решения. За тази цел Експертният център може да се подпомага от един или повече национални координационни центрове или членове на експертната общност в сферата на киберсигурността.

Член 6

Издигане на кандидатури на национални координационни центрове

1. До [дата] всяка държава членка издига кандидатурата на образуванието, което ще изпълнява функцията на национален координационен център за целите на настоящия регламент, и го съобщава на Комисията.
2. Въз основа на оценката относно съответствието на това образувание с критериите, установени в параграф 4, Комисията в рамките на шест месеца от представянето на кандидатурата от държавата членка издава решение за предоставяне на акредитация на образуванието като национален координационен център или за отхвърляне на кандидатурата. Списъкът на националните координационни центрове се публикува от Комисията.
3. Държавите членки могат по всяко време да издигнат кандидатурата на ново образувание за национален координационен център за целите на настоящия регламент. Параграфи 1 и 2 се прилагат за кандидатурата на всяко ново образувание.
4. Предложеният национален координационен център разполага с капацитет да подпомага Експертния център и Мрежата при изпълнението на тяхната мисия, определена в член 3 от настоящия регламент. Той притежава или има пряк достъп до технологичен опит в сферата на киберсигурността и е в състояние ефективно да привлича и да се координира с промишления сектор, публичния сектор и научноизследователската общност.
5. Отношенията между Експертния център и националните координационни центрове се основават на договорно споразумение, подписано между Експертния център и всеки от националните координационни центрове. Споразумението предвижда правилата, уреждащи отношенията и разпределението на задачите между Експертния център и всеки национален координационен център.
6. Мрежата от национални координационни центрове се състои от всички национални координационни центрове, определени от държавите членки.

Член 7

Задачи на националните координационни центрове

1. Националните координационни центрове имат следните задачи:
 - а) да подпомагат Експертния център при постигането на неговите цели и по-специално при координирането на експертната общност в сферата на киберсигурността,
 - б) да улесняват на равнище държави членки участието на отрасъла и другите участници в трансгранични проекти,
 - в) да допринасят съвместно с Експертния център за установяването и справянето със свързаните с киберсигурността предизвикателства, специфични за всеки промишления сектор,
 - г) да изпълняват ролята на звено за контакт на национално равнище за експертната общност в сферата на киберсигурността и Експертния център,
 - д) да се стремят да установят полезните взаимодействия със съответните дейности на национално и регионално равнище,
 - е) да изпълняват конкретните дейности, за които Експертният център е отпуснал безвъзмездни средства, включително чрез предоставяне на финансова подкрепа на трети страни в съответствие с член 204 от Регламент XXX [новия Финансов регламент] при условията, посочени в съответните споразумения за отпускане на безвъзмездни средства,
 - ж) да популяризират и разпространяват на национално и регионално равнище съответните резултати от работата чрез Мрежата, експертната общност в сферата на киберсигурността и Експертния център;
 - з) да оценяват исканията за присъединяване към експертната общност в сферата на киберсигурността от образувания, установени в същата държава членка, в която се намира координационният център.
2. За целите на буква е) финансовата подкрепа за трети страни може да се предоставя под всички форми, посочени в член 125 от Регламент XXX [новия Финансов регламент], включително под формата на еднократни суми.
3. Националните координационни центрове могат да получават безвъзмездни средства от Съюза в съответствие с член 195, буква г) от Регламент XXX [новия Финансов регламент] във връзка с изпълнението на задачите, предвидени в настоящия член.
4. Когато е уместно, националните координационни центрове си сътрудничат чрез Мрежата за изпълнението на задачите, посочени в параграф 1, букви а), б), в), д) и ж).

Член 8

Експертна общност в сферата на киберсигурността

1. Експертната общност в сферата на киберсигурността допринася за осъществяване на мисията на Експертния център, определена в член 3, и увеличава и разпространява експертния опит в областта на киберсигурността в Съюза.

2. Експертната общност в сферата на киберсигурността се състои от промишлени, академични и нестопански научноизследователски организации и от асоциации, както и от публичноправни субекти и други образувания, занимаващи се с оперативни и технически въпроси. Тя обединява основните заинтересовани страни по отношение на технологичния и промишления потенциал в сферата на киберсигурността в Съюза. В нея участват националните координационни центрове, както и институциите и органите на Съюза със съответен експертен опит.
3. Като членове на експертната общност в сферата на киберсигурността могат да бъдат акредитирани само образувания, които са установени на територията на Съюза. Те демонстрират, че разполагат с експертен опит в сферата на киберсигурността по отношение на поне една от следните области:
 - а) научни изследвания;
 - б) промишлени разработки;
 - в) обучение и образование.
4. Експертният център акредитира като членове на експертната общност в сферата на киберсигурността образувания, учредени в съответствие с националното право, след като националният координационен център на държавата членка, в която е установено образуването, извърши оценка на това дали то отговаря на критериите, предвидени в параграф 3. Акредитацията няма срок на валидност, но може да бъде отнета от Експертния център по всяко време, ако той или съответният национален координационен център счита, че образуването не отговаря на критериите, предвидени в параграф 3, или попада в обхвата на съответните разпоредби на член 136 от Регламент XXX [новия Финансов регламент].
5. Експертният център акредитира като членове на експертната общност в сферата на киберсигурността съответните органи, агенции и служби на Съюза, след като извърши оценка на това дали въпросното образование отговаря на критериите, предвидени в параграф 3. Акредитацията няма срок на валидност, но може да бъде отнета от Експертния център по всяко време, ако той счита, че образуването не отговаря на критериите, предвидени в параграф 3, или попада в обхвата на съответните разпоредби на член 136 от Регламент XXX [новия Финансов регламент].
6. Представителите на Комисията могат да участват в дейността на общността.

Член 9

Задачи на членовете на експертната общност в сферата на киберсигурността

Членовете на експертната общност в сферата на киберсигурността:

- 1) подкрепят Експертния център в осъществяването на мисията и целите, определени в членове 3 и 4, и за тази цел си сътрудничат тясно с Експертния център и съответните национални координационни центрове,
- 2) участват в дейностите, насърчавани от Експертния център и националните координационни центрове,

- 3) когато е уместно, участват в работни групи, създадени от управителния съвет на Експертния център, за да изпълняват конкретни дейности, предвидени в работния план на Експертния център;
- 4) когато е уместно, подкрепят Експертния център и националните координационни центрове при популяризирането на конкретни проекти;
- 5) популяризират и разпространяват съответните резултати от дейностите и проектите, осъществени в рамките на общността.

Член 10

Сътрудничество на Експертния център с институции, органи, служби и агенции на Съюза

1. Експертният център сътрудничи със съответните институции, органи, служби и агенции на Съюза, включително Агенцията на Европейския съюз за мрежова и информационна сигурност, екипа за незабавно реагиране при компютърни инциденти в институциите и агенциите на ЕС (CERT-EU), Европейската служба за външна дейност, Съвместния изследователски център на Комисията, Изпълнителната агенция за научни изследвания, Изпълнителната агенция за иновации и мрежи, Европейския център за борба с киберпрестъпността към Европол, както и Европейската агенция по отбрана.
2. Такова сътрудничество се осъществява в рамките на работни договорености. Тези договорености се предоставят на Комисията за предварително одобрение.

ГЛАВА II

ОРГАНИЗАЦИЯ НА ЕКСПЕРТНИЯ ЦЕНТЪР

Член 11

Членство и структура

1. Членовете на Експертния център са Съюзът, представляван от Комисията, и държавите членки.
2. Структурата на Експертния център се състои от:
 - а) управителен съвет, който изпълнява задачите, определени в член 13;
 - б) изпълнителен директор, който изпълнява задачите, определени в член 16;
 - в) промишлен и научен консултативен съвет, който изпълнява функциите, определени в член 20.

РАЗДЕЛ I

УПРАВИТЕЛЕН СЪВЕТ

Член 12

Състав на управителния съвет

1. Управителният съвет се състои от по един представител на всяка държава членка и от петима представители на Комисията от името на Съюза.

2. Всеки член на управителния съвет има заместник, който го представлява при отсъствие.
3. Членовете на управителния съвет и техните заместници се назначават въз основа на познанията им в областта на технологиите, както и на съответните им умения в областта на управлението, администрацията и бюджетирането. Комисията и държавите членки полагат усилия за ограничаване на текучеството на своите представители в управителния съвет, за да се осигури непрекъснатост на работата му. Комисията и държавите членки се стремят към постигането на балансирано представителство между мъже и жени в управителния съвет.
4. Мандатът на членовете на управителния съвет и на техните заместници е четири години. Този мандат подлежи на подновяване.
5. Членовете на управителния съвет действат независимо и по прозрачен начин, в интерес на Експертния център, като защитават неговите цели и мисия, идентичност, автономия и съгласуваност.
6. Комисията може да кани наблюдатели, включително представители на съответни органи, служби и агенции на Съюза, които да участват в заседанията на управителния съвет, според необходимостта.
7. Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) е постоянен наблюдател в управителния съвет.

Член 13

Задачи на управителния съвет

1. Управителният съвет носи цялата отговорност за стратегическата ориентация и функционирането на Експертния център и следи за изпълнението на неговите дейности.
2. Управителният съвет приема правилник за дейността си. Правилникът предвижда конкретни процедури за установяване и избягване на конфликти на интереси и гарантира поверителността на всяка чувствителна информация.
3. Управителният съвет взема необходимите стратегически решения, по-специално:
 - а) приема многогодишен стратегически план, съдържащ изложение на основните приоритети и планираните инициативи на Експертния център, включително оценка на финансовите потребности и на източниците на финансиране;
 - б) приема работния план, годишния финансов отчет и счетоводния баланс и годишния отчет за дейността на Експертния център въз основа на предложение от изпълнителния директор,
 - в) приема специалните финансови правила на Експертния център в съответствие с [член 70 от Финансовия регламент],
 - г) приема процедура за назначаване на изпълнителен директор,
 - д) приеме критериите и процедурите за оценяване и акредитиране на образувания като членове на експертната общност в сферата на киберсигурността,

- е) назначава, освобождава от длъжност, удължава мандата, дава указания и контролира дейността на изпълнителния директор, както и назначава счетоводител,
- ж) приема годишния бюджет на Експертния център, включително съответното щатно разписание с броя на временните длъжности по функционални групи и по степени, броя на договорно наетите служители и командированите национални експерти, изразени в еквивалент на пълно работно време,
- з) приема правила във връзка с конфликти на интереси,
- и) създава работни групи с членовете на експертната общност в сферата на киберсигурността,
- й) назначава членовете на Промишления и научен консултативен съвет,
- к) установява функция по вътрешен одит в съответствие с Делегиран регламент (ЕС) № 1271/2013 на Комисията²⁸,
- л) популяризира дейността на Експертния център в световен мащаб, за да увеличи неговата привлекателност и да го превърне в организация с високи постижения в областта на киберсигурността от световна величина,
- м) определя комуникационната политика на Експертния център по препоръка на изпълнителния директор,
- н) отговаря за наблюдението на подходящи последващи действия във връзка със заключенията от предишни оценки,
- о) определя при необходимост правила за изпълнение на Правилника за длъжностните лица и Условията за работа в съответствие с член 31, параграф 3,
- п) определя, когато е целесъобразно, правила за командироването на национални експерти в Експертния център и за използването на стажанти в съответствие с член 32, параграф 2,
- р) приема правила за сигурност за Експертния център,
- с) приема стратегия за борба с измамите, пропорционална на рисковете от измами, като взема предвид анализа на разходите и ползите от мерките, които трябва да бъдат предприети,
- т) приема методика за изчисляване на финансовите вноски от държавите членки,
- у) отговаря за всяка задача, която не е специално възложена на конкретен орган на Експертния център, може да възлага такива задачи на всяко лице в Експертния център.

Член 14

Председател и заседания на управителния съвет

²⁸

Делегиран регламент (ЕС) № 1271/2013 на Комисията от 30 септември 2013 г. относно рамковия Финансов регламент за органите, посочени в член 208 от Регламент (ЕС, Евратом) № 966/2012 на Европейския парламент и на Съвета (ОВ L 328, 7.12.2013 г., стр. 42.)

1. Управителният съвет избира председател и заместник-председател измежду членовете с право на глас за период от две години. Мандатът на председателя и на заместник-председателя може да бъде удължен еднократно след решение на управителния съвет. Ако обаче по време на мандата им те престанат да бъдат членове на управителния съвет, мандатът изтича автоматично на същата дата. Заместник-председателят замества служебно председателя, ако последният не е в състояние да изпълнява своите задължения. Председателят участва в гласуването.
2. Управителният съвет провежда редовни заседания най-малко три пъти годишно. Той може да провежда извънредни заседания по искане на Комисията, по искане на една трета от всички свои членове, по искане на председателя или по искане на изпълнителния директор във връзка с изпълнението на задачите му.
3. Изпълнителният директор участва в обсъжданията, освен ако управителният съвет не реши друго, но няма право на глас. Управителният съвет може да покани, според конкретния случай, други лица да присъстват на неговите заседания като наблюдатели.
4. По покана на председателя членове на Промисления и научен консултативен съвет могат да участват в заседанията на управителния съвет без право на глас.
5. Членовете на управителния съвет и техните заместници могат, при спазване на неговия правилник за дейността, да бъдат подпомагани на заседанията от съветници или експерти.
6. Експертният център осигурява секретариата на управителния съвет.

Член 15

Правила за гласуване в управителния съвет

1. Съюзът разполага с 50 % от правата на глас. Правата на глас на Съюза са неделими.
2. Всяка участваща държава членка разполага с един глас.
3. Управителният съвет взема своите решения с мнозинство от най-малко 75 % от всички гласове, включително гласовете на членовете, които не присъстват, представляващи най-малко 75 % от общия размер на финансовите вноски за Експертния център. Финансовата вноска ще се изчислява въз основа на прогнозните разходи, предложени от държавите членки, посочени в член 17, параграф 2, буква в), и въз основа на доклада за стойността на вноските от участващите държави членки, посочен в член 22, параграф 5.
4. Права на глас притежават единствено представителите на Комисията и представителите на участващите държави членки.
5. Председателят участва в гласуването.

РАЗДЕЛ II

ИЗПЪЛНИТЕЛЕН ДИРЕКТОР

Член 16

Назначаване, освобождаване от длъжност или удължаване на мандата на изпълнителния директор

1. Изпълнителният директор е лице, което притежава експертен опит и се ползва с добро име в областите на дейност на Експертния център.
2. Изпълнителният директор се назначава като срочно нает служител на Експертния център съгласно член 2, буква а) от Условиата за работа на другите служители.
3. Управителният съвет назначава изпълнителния директор от списък с кандидати, предложени от Комисията, след открита и прозрачна процедура за подбор.
4. За целите на сключването на договора на изпълнителния директор Експертният център се представлява от председателя на управителния съвет.
5. Мандатът на изпълнителния директор е четири години. Към края на този период Комисията извършва оценка, която взема предвид оценката на работата на изпълнителния директор и бъдещите цели и предизвикателства пред Експертния център.
6. По предложение на Комисията, което взема предвид оценката, посочена в параграф 5, управителният съвет може еднократно да удължи мандата на изпълнителния директор с не повече от четири години.
7. Изпълнителен директор, чийто мандат е бил удължен, не може да участва в нова процедура за подбор за същата длъжност.
8. Изпълнителният директор се отстранява от длъжност единствено с решение на управителния съвет по предложение на Комисията.

Член 17

Задачи на изпълнителния директор

1. Изпълнителният директор отговаря за дейността и ежедневното управление на Експертния център и е неговият законен представител. Изпълнителният директор отговаря пред управителния съвет и изпълнява своите задължения при условията на пълна независимост в рамките на възложените му правомощия.
2. Изпълнителният директор, по-специално, осъществява по независим начин следните задачи:
 - а) изпълнява решенията, приети от управителния съвет,
 - б) подпомага управителния съвет в неговата работа, осигурява секретариат за неговите заседания и доставя цялата необходима информация за изпълнението на неговите задължения,
 - в) след консултации с управителния съвет и Комисията, изготвя и внася за приемане от управителния съвет проекта на многогодишен стратегически план и проекта на годишен работен план на Експертния център, включително обхвата на поканите за представяне на предложения, поканите за изразяване на интерес и поканите за участие в търг, които са необходими за изпълнението на работния план, и съответните прогнози за размера на разходите, предложени от държавите членки и Комисията,
 - г) изготвя и внася за приемане от управителния съвет проекта за годишен бюджет, включително съответното щатно разписание с броя на

временните длъжности по функционални групи и по степени, броя на договорно наетите служители и командированите национални експерти, изразени в еквивалент на пълно работно време,

- д) изпълнява работния план и докладва пред управителния съвет за изпълнението му,
- е) изготвя проекта на годишен отчет за дейността на Експертния център, включително информацията относно съответните разходи,
- ж) осигурява прилагането на ефективни процедури за мониторинг и оценка във връзка с работата на Експертния център,
- з) изготвя план за действие за съобразяване със заключенията от оценки за изминал период и докладва за напредъка на всеки две години пред Комисията,
- и) изготвя, договаря и сключва споразумения с националните координационни центрове,
- й) носи отговорност за административните и финансовите въпроси и въпросите, свързани с управлението на персонала, включително изпълнението на бюджета на Експертния център, като се съобразява с получените консултации от функцията по вътрешен одит, в рамките на правомощията, делегирани му от управителния съвет,
- к) одобрява и управлява, в съответствие с работния план, откриването на покани за представяне на предложения и администрира споразуменията и решенията за отпускане на безвъзмездни средства,
- л) одобрява списъка от действия, избрани за финансиране въз основа на класация, която е изготвена от комисия от независими експерти,
- м) одобрява и управлява, в съответствие с работния план, откриването на покани за участие в търг и администрира договорите,
- н) одобрява офертите, избрани за финансиране,
- о) представя проекта на годишен финансов отчет и счетоводен баланс на функцията по вътрешен одит и в следствие на управителния съвет,
- п) осигурява извършването на оценка на риска и управление на риска,
- р) подписва отделните споразумения, решения и договори за отпускане на безвъзмездни средства,
- с) подписва договорите за обществени поръчки,
- т) изготвя план за последващи действия във връзка със заключенията от вътрешните или външните одитни доклади, както и от разследвания на Европейската служба за борба с измамите (OLAF), и представя доклади за напредъка два пъти годишно на Комисията и редовно на управителния съвет,
- у) изготвя проект на финансовите правила, приложими по отношение на Експертния център;
- ф) създава и осигурява функционирането на ефективна и ефикасна система за вътрешен контрол и докладва на управителния съвет за всяка значителна промяна в нея,

- х) осигурява ефективна комуникация с институциите на Съюза,
- ц) предприема всякакви други мерки, необходими за оценката на напредъка на Експертния център по постигане на мисията и целите му, предвидени в членове 3 и 4 от настоящия регламент,
- ч) изпълнява всички други задачи, възложени или делегирани от управителния съвет.

РАЗДЕЛ III

ПРОМИШЛЕН И НАУЧЕН КОНСУЛТАТИВЕН СЪВЕТ

Член 18

Състав на Промисления и научен консултативен съвет

1. Промисленият и научен консултативен съвет е съставен от най-много шестнадесет членове. Членовете се назначават от управителния съвет измежду представителите на образуванията от експертната общност в сферата на киберсигурността.
2. Членовете на Промисления и научен консултативен съвет притежават експертен опит по отношение на научните изследвания, промишлените разработки, професионалните услуги, свързани с киберсигурността, или по отношение на тяхното внедряване. Изискванията за такъв експертен опит се определят допълнително от управителния съвет.
3. Дейността на консултативния съвет, както и процедурите за назначаване на членовете му от управителния съвет се определят в правилника за дейността на Експертния център и се оповестяват публично.
4. Мандатът на членовете на Промисления и научен консултативен съвет е три години. Този мандат подлежи на подновяване.
5. Представителите на Комисията и на Агенцията на Европейския съюз за мрежова и информационна сигурност могат да участват в работата на Промисления и научен консултативен съвет и да я подпомагат.

Член 19

Функции на Промисления и научен консултативен съвет

1. Промисленият и научен консултативен съвет заседава най-малко два пъти годишно.
2. Промисленият и научен консултативен съвет може да консултира управителния съвет относно създаването на работни групи по конкретни въпроси, свързани с работата на Експертния център, като при необходимост общата координация се осъществява от един или повече членове на Промисления и научен консултативен съвет.
3. Промисленият и научен консултативен съвет избира своя председател.
4. Промисленият и научен консултативен съвет приема своя правилник за дейността, включително издигането на кандидатури на представителите, които ще го представляват в необходимите случаи, и продължителността на тяхното представителство.

Задачи на Промисления и научен консултативен съвет

Промисленият и научен консултативен съвет консултира Експертния център по отношение на изпълнението на неговите дейности и:

- 1) предоставя на изпълнителния директор и на управителния съвет стратегически съвети и принос за изготвянето на работния план и многогодишния стратегически план в сроковете, определени от управителния съвет;
- 2) организира обществени консултации, отворени за всички заинтересовани страни от публичния и частния сектор, които имат интереси в областта на киберсигурността, с цел събиране на информация за стратегическите съвети, посочени в параграф 1;
- 3) насърчава предоставянето и събира обратна информация относно работния план и многогодишния стратегически план на Експертния център.

ГЛАВА III

ФИНАНСОВИ РАЗПОРЕДБИ

Финансова вноска от Съюза

1. Финансовата вноска от Съюза за покриване на административните и оперативните разходи на Експертния център включва следното:
 - а) 1 981 668 000 евро от програмата „Цифрова Европа“, включително до 23 746 000 евро за административни разходи,
 - б) сума от програмата „Хоризонт Европа“, включително за административни разходи, която да бъде определена, като се взема предвид процесът на стратегическо планиране, който следва да се изпълнява в съответствие с член 6, параграф 6 от Регламент XXX [Регламента за „Хоризонт Европа“].
2. Максималната финансова вноска от Съюза се плаща от бюджетните кредити в общия бюджет на Съюза, определени за осъществяване на [програмата „Цифрова Европа“] и на специалната програма за изпълнение на „Хоризонт Европа“, създадена с Решение XXX.
3. Експертният център изпълнява действията в областта на киберсигурността по [програма „Цифрова Европа“] и [програма „Хоризонт Европа“] в съответствие с член 62, буква в), подточка iv) от Регламент (ЕС, Евратом) № XXX²⁹ [Финансовия регламент].
4. Финансовата вноска от Съюза не покрива задачите, посочени в член 4, параграф 8, буква б).

²⁹ [Да се добавят пълното заглавие и номерът в Официален вестник]

Член 22

Финансова вноска от участващите държави членки

1. Участващите държави членки предоставят финансова вноска за покриване на оперативните и административните разходи на Експертния център на обща стойност, равна най-малко на сумите, посочени в член 21, параграф 1 от настоящия регламент.
2. За целите на оценката на вноските, посочени в параграф 1 и в член 23, параграф 3, буква б), подточка ii), разходите се определят в съответствие с обичайните практики за осчетоводяване на разходите на съответните държави членки, приложимите счетоводни стандарти на държавата членка и приложимите международни счетоводни стандарти и международни стандарти за финансово отчитане. Разходите се заверяват от независим външен одитор, назначен от съответната държава членка. Методът на остойностяване може да бъде проверен от Експертния център, ако е налице неяснота при извършената заверка.
3. Ако участваща държава членка не изпълнява поетите задължения във връзка с финансовата си вноска, изпълнителният директор излага това обстоятелство в писмена форма и определя приемлив срок за изпълнение на поетото задължение. Ако ангажиментът не бъде изпълнен в определения срок, изпълнителният директор свиква заседание на управителния съвет, който да реши дали да бъде отнето правото на глас на неизправната участваща държава членка или да бъдат взети други мерки, докато този неин ангажимент не бъде изпълнен. Правата на глас на неизправната държава членка се преустановяват до изпълнение на нейните ангажименти.
4. Комисията може да прекрати, пропорционално да намали или да преустанови финансовата вноска на Съюза в Експертния център, ако участващите държави членки не изплащат вноските, посочени в параграф 1 от настоящия член, или ги изплащат частично или със закъснение.
5. Най-късно до 31 януари всяка година участващите държави членки докладват на управителния съвет стойността на посочените в параграф 1 вноски, направени през всяка от предходните финансови години.

Член 23

Разходи и ресурси на Експертния център

1. Експертният център се финансира съвместно от Съюза и държавите членки чрез финансов принос, изплащан на вноски, и принос, състоящ се в покриване на разходите, направени от националните координационни центрове и бенефициерите при изпълнението на дейностите, който не се възстановява от Експертния център.
2. Административните разходи на Експертния център не трябва да превишават [число] евро и се покриват от финансови вноски, разделени поравно на годишна основа между Съюза и участващите държави членки. Ако част от вноската за административни разходи остане неизползвана, тя може да бъде предоставена за покриване на оперативните разходи на Експертния център.
3. Оперативните разходи на Експертния център се покриват от:

- а) финансовата вноска от Съюза;
 - б) вноските от участващите държави членки под формата на:
 - i) финансови вноски, както и
 - ii) когато е уместно, непарични вноски от участващите държави членки за покриване на разходите, извършени от националните координационни центрове и бенефициерите за изпълнението на непреки действия, като се приспадне участието на Експертния център и всяко друго участие на Съюза в тези разходи.
4. Ресурсите на Експертния център, вписани в неговия бюджет, се състоят от следните елементи:
- а) финансовите вноски на участващите държави членки за покриване на административните разходи,
 - б) финансовите вноски на участващите държави членки за покриване на оперативните разходи,
 - в) всички приходи, реализирани от Експертния център,
 - г) всички други финансови вноски, средства и приходи.
5. Лихвата, начислена върху вноските, плащани за Експертния център от участващите държави членки, се счита за негов приход.
6. Всички ресурси на Експертния център и неговите дейности се използват за постигане на целите, предвидени в член 4.
7. Експертният център е собственик на всички активи, създадени от него или прехвърлени му за изпълнението на неговите цели.
8. Освен при ликвидация на Експертния център, всички приходи, надвишаващи разходите, не се изплащат на членовете на Експертния център.

Член 24

Финансови ангажименти

Финансовите ангажименти на Експертния център не надхвърлят размера на финансовите средства, които са в наличност или за които са поети бюджетни задължения от членовете.

Член 25

Финансова година

Финансовата година започва на 1 януари и приключва на 31 декември.

Член 26

Съставяне на бюджета

1. Всяка година изпълнителният директор изготвя проект на разчета за предвидените приходи и разходи на Експертния център за следващата финансова година и го изпраща на управителния съвет заедно с проект на щатното разписание. Приходите и разходите са балансирани. Разходите на Експертния център включват разходите за персонала, административните,

инфраструктурните и оперативните разходи. Административните разходи се свеждат до минимум.

2. Въз основа на проекта на разчета за предвидените приходи и разходи, посочен в параграф 1, управителният съвет ежегодно изготвя разчет за предвидените приходи и разходи на Експертния център за следващата финансова година.
3. До 31 януари всяка година управителният съвет изпраща разчета за предвидените приходи и разходи, посочен в параграф 2, който е част от проекта на единен програмен документ, на Комисията.
4. Въз основа на този разчет Комисията включва в проекта за бюджет на Съюза прогнозните средства, които прецени за необходими за щатното разписание, и размера на вноската, която се заделя от общия бюджет, и ги представя на Европейския парламент и на Съвета в съответствие с членове 313 и 314 от ДФЕС.
5. Европейският парламент и Съветът разрешават отпускане на бюджетни кредити за вноската в Експертния център.
6. Европейският парламент и Съветът приемат щатното разписание на Експертния център.
7. Заедно с работния план управителният съвет приема бюджета на Експертния център. Той става окончателен след окончателното приемане на общия бюджет на Съюза. Когато е уместно, управителният съвет коригира бюджета и работния план на Експертния център в съответствие с общия бюджет на Съюза.

Член 27

Представяне на отчетите на Експертния център и освобождаване от отговорност във връзка с изпълнението на бюджета

Представянето на предварителните и окончателните отчети на Експертния център и освобождаването от отговорност във връзка с изпълнението на бюджета се извършват при спазване на правилата и сроковете, предвидени във Финансовия регламент и във финансовите правила на Експертния център, приети в съответствие с член 29.

Член 28

Доклади за дейността и финансови отчети

1. Всяка година изпълнителният директор докладва на управителния съвет за изпълнението на своите задължения в съответствие с финансовите правила на Експертния център.
2. В срок от два месеца след приключването на всяка финансова година изпълнителният директор представя за одобрение от управителния съвет годишен отчет за дейността относно напредъка на Експертния център през предходната календарна година, по-специално по отношение на работния план за тази година. Наред с другото, този доклад включва информацията относно следните въпроси:
 - а) извършените оперативни дейности, както и съответните разходи,
 - б) представените дейности, включително разбивка по видове участници, в това число МСП, и по държави членки,

- в) избраните за финансиране дейности, включително разбивка по видове участници, в това число МСП, и по държави членки, като се посочва вноската на Експертния център за отделните участници и дейности,
 - г) напредъка към постигането на целите, посочени в член 4, и предложения за необходимата по-нататъшна работа за постигане на тези цели.
3. След като бъде одобрен от управителния съвет, годишният отчет за дейността става обществено достояние.

Член 29

Финансови правила

Експертният център приема свои специфични финансови правила в съответствие с член 70 от Регламент XXX [новия Финансов регламент].

Член 30

Защита на финансовите интереси

1. Експертният център взема подходящи мерки, за да гарантира, че при изпълнението на финансираните съгласно настоящия регламент дейности финансовите интереси на Съюза са защитени чрез прилагането на превантивни мерки срещу измами, корупция и всякакви други незаконни действия, чрез ефективни проверки, а ако се открият нередности — чрез събиране на недължимо платените суми, и ако е целесъобразно — посредством ефективни, пропорционални и възпиращи административни санкции.
2. Експертният център предоставя на служителите на Комисията и други упълномощени от Комисията лица, както и на Сметната палата, достъп до своите обекти и помещения и до цялата информация, включително информация в електронен формат, която е необходима за извършване на техните одити.
3. Европейската служба за борба с измамите (OLAF) може да извършва разследвания, включително проверки и инспекции на място, в съответствие с разпоредбите и процедурите, установени в Регламент (Евратом, ЕО) № 2185/96 на Съвета³⁰ и Регламент (ЕС, Евратом) № 883/2013 на Европейския парламент и на Съвета³¹, за да се установи дали е налице измама, корупция или друга незаконна дейност, накърняваща финансовите интереси на Съюза, във връзка със споразумение за отпускане на безвъзмездни или договор, финансирани пряко или непряко съгласно настоящия регламент.
4. Без да се засягат параграфи 1, 2 и 3 от настоящия член, договорите и споразуменията за отпускане на безвъзмездни средства в резултат от изпълнението на настоящия регламент съдържат разпоредби, които изрично

³⁰ Регламент (Евратом, ЕО) № 2185/96 на Съвета от 11 ноември 1996 г. относно контрола и проверките на място, извършвани от Комисията за защита на финансовите интереси на Европейските общности срещу измами и други нередности (ОВ L 292, 15.11.1996 г., стр. 2).

³¹ Регламент (ЕС, Евратом) № 883/2013 на Европейския парламент и на Съвета от 11 септември 2013 г. относно разследванията, провеждани от Европейската служба за борба с измамите (OLAF), и за отмяна на Регламент (ЕО) № 1073/1999 на Европейския парламент и на Съвета и Регламент (Евратом) № 1074/1999 на Съвета (ОВ L 248, 18.9.2013 г., стр. 1–22).

упълномощават Комисията, Експертния център, Сметната палата и OLAF да извършват такива одити и разследвания в съответствие с тяхната компетентност. Когато изпълнението на дадено действие е възложено на външен изпълнител или е налице цялостно или частично прехвърляне на пълномощията, или когато изпълнението изисква възлагането на договор за обществена поръчка или предоставянето на финансова подкрепа на трета страна, в договора или споразумението за отпускане на безвъзмездни средства се включва задължение за изпълнителя или бенефициера да наложи на съответната трета страна изрично да приеме тези правомощия на Комисията, Експертния център, Сметната палата и OLAF.

ГЛАВА IV

ПЕРСОНАЛ НА ЕКСПЕРТНИЯ ЦЕНТЪР

Член 31

Персонал

1. По отношение на персонала на Експертния център се прилагат Правилникът за длъжностните лица на Европейския съюз и Условието за работа на другите служители на Съюза, установени с Регламент (ЕИО, Евратом, ЕОБС) № 259/68³² (по-нататък наричани „Правилник за длъжностните лица“ и „Условия за работа“), и правилата, приети съвместно от институциите на Съюза за целите на прилагането на посочените Правилник за длъжностните лица и Условия за работа.
2. По отношение на персонала на Експертния център управителният съвет упражнява правомощията, предоставени на органа по назначаването съгласно Правилника за длъжностните лица, както и тези, предоставени на органа, оправомощен да сключва договори, съгласно Условията за работа („правомощия на органа по назначаването“).
3. Управителният съвет приема в съответствие с член 110 от Правилника за длъжностните лица решение на основата на член 2, параграф 1 от Правилника за длъжностните лица и на член 6 от Условията за работа относно делегирането на съответните правомощия на органа по назначаване на изпълнителния директор и определянето на условията, при които делегирането може да бъде прекратено. Изпълнителният директор има правото от своя страна да прехвърли тези правомощия на други лица.
4. При извънредни обстоятелства управителният съвет може със свое решение временно да прекрати делегирането на правомощията на орган по назначаване на изпълнителния директор и съответно на прехвърлените от него правомощия. В такива случаи самият управителен съвет упражнява правомощията на органа по назначаване или ги делегира на някой от своите членове или на някой служител на Експертния център, различен от изпълнителния директор.

³² Регламент (ЕИО, Евратом, ЕОБС) № 259/68 на Съвета от 29 февруари 1968 г. относно определяне на Правилника за длъжностните лица и Условията за работа на другите служители на Европейските общности и относно постановяване на специални мерки, временно приложими за длъжностни лица на Комисията (ОВ L 56, 4.3.1968 г., стр. 1).

5. Управителният съвет приема правила за изпълнение на Правилника за длъжностните лица и Условията за работа в съответствие с член 110 от Правилника за длъжностните лица.
6. Числеността на персонала се определя в щатното разписание на Експертния център, в съответствие с неговия годишен бюджет, като се посочва броят на временните длъжности по функционални групи и по степени, както и броят на договорно наетите служители, изразени в еквивалент на пълно работно време.
7. Персоналът на Експертния център се състои от временно наети служители и договорно наети служители.
8. Всички разходи във връзка с персонала се поемат от Експертния център.

Член 32

Командировани национални експерти и друг персонал

1. Експертният център може да използва командировани национални експерти или друг персонал, който не е нает от Експертния център.
2. Управителният съвет приема решение за определяне на правила за командироването на национални експерти в Експертния център, със съгласието на Комисията.

Член 33

Привилегии и имунитети

Към Експертния център и неговия персонал се прилага Протокол № 7 за привилегиите и имунитетите на Европейския съюз, приложен към Договора за Европейския съюз и към Договора за функционирането на Европейския съюз.

ГЛАВА V

ОБЩИ РАЗПОРЕДБИ

Член 34

Правила за сигурност

1. Член 12, параграф 7 от Регламент (ЕС) № XXX [програма „Цифрова Европа“] се прилага за участието във всички дейности, финансирани от Експертния център.
2. За дейностите, финансирани от „Хоризонт Европа“, се прилагат следните специфични правила за сигурност:
 - а) за целите на член 34, параграф 1 [Собственост и защита] от Регламент (ЕС) № XXX [Хоризонт Европа], когато е предвидено в работния план, предоставянето на неизключителни лицензи може да бъде ограничено до трети страни, които са установени или се счита, че са установени в държави членки и се контролират от държави членки и/или граждани на държави членки;
 - б) за целите на член 36, параграф 4, буква б) [Прехвърляне и лицензиране] от Регламент (ЕС) № XXX [„Хоризонт Европа“] прехвърлянето или

лицензирането на резултати на правен субект, установен в асоциирана държава или установен в Съюза, но контролиран от трети държави, също е основание за възражение срещу прехвърлянето на собствеността върху резултатите или срещу предоставянето на изключителен лиценз във връзка с резултатите;

- в) за целите на член 37, параграф 3, буква а) [Права на достъп] от Регламент (ЕС) № XXX [„Хоризонт Европа“], когато е предвидено в работния план, предоставянето на достъп до резултатите и до предходните знания може да бъде ограничено само до правен субект, който е установен или се счита, че е установен в държави членки и се контролира от държави членки и/или граждани на държави членки.

Член 35

Прозрачност

1. Експертният център извършва дейността си при висока степен на прозрачност.
2. Експертният център гарантира, че на обществеността и на заинтересованите страни се предоставя целесъобразна, обективна, достоверна и леснодостъпна информация, по-специално по отношение на резултатите от неговата дейност. Освен това той оповестява публично декларациите за интереси, направени в съответствие с член 41.
3. По предложение на изпълнителния директор управителният съвет може да разреши на заинтересовани страни да наблюдават работата по някои от дейностите на Експертния център.
4. Експертният център установява във правилник за дейността си практическите ред и условия за прилагане на правилата за прозрачност, посочени в параграфи 1 и 2. За дейности, финансирани по линия на „Хоризонт Европа“, в тях надлежно се вземат предвид разпоредбите в приложение III към Регламента за „Хоризонт Европа“.

Член 36

Правила за сигурност относно защитата на класифицирана информация и на неклассифицирана чувствителна информация

1. Без да се засяга член 35, Експертният център няма право да разкрива на трети страни информация, която обработва или получава, за която е отправено обосновано искане за поверително цялостно или частично обработване.
2. Членовете на управителния съвет, изпълнителният директор, членовете на Промисления и научен консултативен съвет, участващите в работните ad hoc групи външни експерти и членовете на персонала на центъра са задължени да спазват изискванията за поверителност съгласно член 339 от Договора за функционирането на Европейския съюз, дори и след приключване на службата им.
3. Управителният съвет на Експертния център приема след одобрение от Комисията правилата за сигурност на центъра въз основа на принципите и правилата, заложи в правилата за сигурност на Комисията за защита на класифицираната информация на Европейския съюз (КИЕС) и чувствителната неклассифицирана информация, *inter alia*, разпоредбите за обработката и

съхранението на такава информация, предвидени в решения (ЕС, Евратом) 2015/443³³ и 2015/444³⁴ на Комисията.

4. Експертният център може да предприема всички необходими мерки за улесняване на обмена с Комисията и държавите членки и, когато е целесъобразно — с компетентните агенции и органи на Съюза, на информация, която е от значение за неговите задачи. Всяка сключена за тази цел административна договореност относно споделянето на КИЕС или, при отсъствие на такава договореност, всяко извънредно *ad hoc* предоставяне на КИЕС се осъществяват след предварителното одобрение на Комисията.

Член 37

Достъп до документи

1. По отношение на документите, съхранявани от Експертния център, се прилага Регламент (ЕО) № 1049/2001.
2. Управителният съвет приема реда за прилагането на Регламент (ЕО) № 1049/2001 в срок до шест месеца от създаването на Експертния център.
3. Срещу решенията, взети от Експертния център съгласно член 8 от Регламент (ЕО) № 1049/2001, може да се подава жалба до омбудсмана по реда и при условията на член 228 от Договора за функционирането на Европейския съюз или те може да се обжалват пред Съда на Европейския съюз по реда и при условията на член 263 от Договора за функционирането на Европейския съюз.

Член 38

Мониторинг, оценка и преразглеждане

1. Експертният център гарантира, че неговите дейности, включително онези, които се управляват чрез националните координационни центрове и Мрежата, са предмет на постоянен и систематичен мониторинг и периодична оценка. Експертният център гарантира, че данните за изпълнението на програмата за мониторинг и резултатите от нея се събират по ефикасен, ефективен и своевременен начин и на получателите на средства от Съюза и държавите членки се налагат пропорционални изисквания за докладване. Резултатите от оценката се огласяват.
2. След като се събере достатъчна налична информация относно прилагането на настоящия регламент, но не по-късно от три и половина години след началото на прилагането му, Комисията извършва междинна оценка на Експертния център. Комисията изготвя доклад относно тази оценка и го представя пред Европейския парламент и Съвета до 31 декември 2024 г. Експертният център и държавите членки предоставят на Комисията информацията, необходима за изготвяне на този доклад.
3. Оценката, посочена в параграф 2, включва и оценка на резултатите, постигнати от Експертния център, като се вземат предвид неговите цели, мандат и задачи.

³³ Решение (ЕС, Евратом) 2015/443 на Комисията от 13 март 2015 г. относно сигурността в Комисията (ОВ L 72, 17.3.2015 г., стр. 41).

³⁴ Решение (ЕС, Евратом) 2015/444 на Комисията от 13 март 2015 г. относно правилата за сигурност за защита на класифицираната информация на ЕС (ОВ L 72, 17.3.2015 г., стр. 53).

Ако Комисията счете, че продължаването на съществуването на Експертния център е обосновано по отношение на поставените му цели, мандат и задачи, тя може да предложи удължаване на мандата на Експертния център, установен в член 46.

4. Въз основа на заключенията от междинната оценка, посочена в параграф 2, Комисията може да предприеме действия в съответствие с [член 22, параграф 5] или всякакви други подходящи действия.
5. Мониторингът, оценката, постепенното прекратяване на финансирането и възобновяването на вноската от програма „Хоризонт Европа“ ще се осъществяват в съответствие с разпоредбите на членове 8, 45 и 47 и приложение III към Регламента за „Хоризонт Европа“ и договорените условия и ред за изпълнение.
6. Мониторингът, докладването и оценката на финансовата вноска от програма „Цифрова Европа“ ще се осъществяват в съответствие с разпоредбите на членове 24 и 25 от програмата „Цифрова Европа“.
7. В случай на ликвидация на Експертния център Комисията ще извърши окончателна оценка на Експертния център в рамките на шест месеца след ликвидацията, но не по-късно от две години след задействането на процедурата по ликвидация, предвидена в член 46 от настоящия регламент. Резултатите от окончателната оценка се представят на Европейския парламент и на Съвета.

Член 39

Отговорност на Експертния център

1. Договорната отговорност на Експертния център се урежда от правото, приложимо към съответното споразумение, решение или договор.
2. В случай на извъндоговорна отговорност Експертният център действа в съответствие с основните принципи, общи за правните системи на държавите членки, и поправя всички вреди, причинени от неговия персонал при изпълнението на задълженията му.
3. Всички плащания от Експертния център във връзка с посочените в параграфи 1 и 2 задължения и направените разходи и разноси във връзка с тях се считат за разходи на Експертния център и се покриват от неговите средства.
4. Експертният център носи цялата отговорност за изпълнението на своите задължения.

Член 40

Компетентност на Съда на Европейския съюз и приложимо право

1. Съдът на Европейския съюз е компетентен:
 - 1) съгласно арбитражни клаузи, съдържащи се в сключени от Експертния център споразумения, решения или договори;
 - 2) при спорове, свързани с компенсация на вреди, причинени от членовете на персонала на Експертния център при изпълнение на техните задължения;

- 3) по всякакви спорове между Експертния център и неговите служители в границите и при условията, определени в Правилника за длъжностните лица.
2. По всички въпроси, които не са обхванати от настоящия регламент или друг акт от правото на Съюза, се прилага правото на държавата членка, в която се намира седалището на Експертния център.

Член 41

Отговорност на членовете и застраховка

1. Финансовата отговорност на членовете за дългове на Експертния център се ограничава до вече направената от тях вноска за административните разходи.
2. Експертният център сключва и поддържа подходяща застраховка.

Член 42

Конфликти на интереси

Управителният съвет на Експертния център приема правила за недопускане и управление на конфликти на интереси по отношение на неговите членове, органи и персонал. В тези правила се предвиждат разпоредби за избягване на конфликт на интереси по отношение на представителите на членовете, участващи в управителния съвет и в Промисления и научен консултативен съвет, в съответствие с Регламент XXX [новия Финансов регламент].

Член 43

Защита на личните данни

1. Обработването на лични данни от страна на Експертния център е предмет на Регламент (ЕС) № XXX/2018 на Европейския парламент и на Съвета.
2. Управителният съвет приема мерките по прилагане, посочени в член xx, параграф 3 от Регламент (ЕС) № xxx/2018. Управителният съвет може да приеме допълнителни мерки, необходими за прилагането на Регламент (ЕС) № xxx/2018 от Експертния център.

Член 44

Подпомагане от приемащата държава членка

Може да се сключи административно споразумение между Експертния център и държавата членка [Белгия], в която се намира седалището му, относно привилегиите и имунитетите, както и относно друга подкрепа, която тази държава членка предоставя на Експертния център.

ГЛАВА VII

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 45

Първоначални действия

1. Комисията отговаря за създаването и първоначалната дейност на Експертния център, докато той придобие оперативен капацитет да изпълнява собствения си бюджет. В съответствие с правото на Съюза Комисията извършва всички необходими действия с участието на компетентните органи от Експертния център.
2. За целите на параграф 1, докато изпълнителният директор поеме функциите си, след като е бил назначен от управителния съвет в съответствие с член 16, Комисията може да назначи временно изпълняващ длъжността изпълнителен директор, който да изпълнява функциите на изпълнителен директор и който може да бъде подпомаган от ограничен брой служители от Комисията. Комисията може да предостави временно ограничен брой свои служители.
3. Временно изпълняващият длъжността изпълнителен директор има право да разрешава всички плащания, извършвани с бюджетните кредити, предвидени в годишния бюджет на Експертния център, след като тези плащания бъдат одобрени от управителния съвет, и може да сключва споразумения, решения и договори, включително договори за наемане на персонал, след приемането на шатното разписание на Експертния център.
4. Временно изпълняващият длъжността изпълнителен директор определя по общо съгласие с изпълнителния директор на Експертния център и след одобрението на управителния съвет датата, на която Експертният център ще има капацитет да изпълнява собствения си бюджет. Считано от тази дата, Комисията се въздържа от поемане на задължения и извършване на плащания за дейностите на Експертния център.

Член 46

Продължителност на съществуване

1. Експертният център се създава за периода от 1 януари 2021 г. до 31 декември 2029 г.
2. В края на този период се задейства процедура по ликвидация, освен ако не бъде решено друго чрез преразглеждане на настоящия регламент. Процедурата по ликвидация се задейства автоматично, ако Съюзът или всички участващи държави членки се оттеглят от Експертния център.
3. За целите на процедурата по ликвидация на Експертния център управителният съвет назначава един или повече ликвидатори, които изпълняват решенията на управителния съвет.
4. Когато Експертният център се ликвидира, неговите активи се използват за покриване на неговите пасиви и на разходите във връзка с ликвидацията. Всеки наличен излишък се разпределя между Съюза и участващите държави членки

пропорционално на тяхната финансова вноска в Експертния център. Остатъкът, разпределен по такъв начин на Съюза, се връща в бюджета на Съюза.

Член 47

Влизане в сила

Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на [...] година.

За Европейския парламент
Председател

За Съвета
Председател

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

- 1.1. Наименование на предложението/инициативата
- 1.2. Съответни области на политиката в структурата на УД/БД
- 1.3. Естество на предложението/инициативата
- 1.4. Цели
- 1.5. Мотиви за предложението/инициативата
- 1.6. Срок на действие и финансово отражение
- 1.7. Планирани методи на управление

2. МЕРКИ ЗА УПРАВЛЕНИЕ

- 2.1. Правила за мониторинг и докладване
- 2.2. Система за управление и контрол
- 2.3. Мерки за предотвратяване на измами и нередности

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

- 3.1. Съответни функции от многогодишната финансова рамка и разходни бюджетни редове
- 3.2. Очаквано отражение върху разходите
 - 3.2.1. *Обобщение на очакваното отражение върху разходите*
 - 3.2.2. *Очаквано отражение върху бюджетните кредити за оперативни разходи*
 - 3.2.3. *Очаквано отражение върху бюджетните кредити за административни разходи*
 - 3.2.4. *Съвместимост с настоящата многогодишна финансова рамка*
 - 3.2.5. *Финансов принос от трети страни*
- 3.3. Очаквано отражение върху приходите

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

Регламент за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността

1.2. Съответни области на политиката в структурата на УД/БД³⁵

Научни изследвания и иновации
Европейски стратегически инвестиции

1.3. Естество на предложението/инициативата

- ☒ Предложението/инициативата е във връзка с **ново действие**
- ☐ Предложението/инициативата е във връзка с **ново действие след пилотен проект/подготвително действие**³⁶
- ☐ Предложението/инициативата е във връзка с **продължаване на съществуващо действие**
- ☐ Предложението/инициативата е във връзка с **действие, пренасочено към ново действие**

1.4. Цели

1.4.1. Многогодишни стратегически цели на Комисията, за чието изпълнение е предназначено предложението/инициативата

1. Свързан цифров единен пазар
2. Нов стимул за работни места, растеж и инвестиции

1.4.2. Специфични цели, за които се отнася предложението/инициативата

Специфични цели

1.3 Цифровата икономика може да разгърне пълния си потенциал, подкрепена от инициативи, които дават възможност за пълно развитие на цифровите технологии и технологиите за данни.

2.1 Европа запазва позицията си на световен лидер в цифровата икономика, която предоставя на европейските предприятия възможност за растеж в световен мащаб въз основа на силно предприемачество в областта на цифровите технологии и ефективни нововъзникващи предприятия, а на промишления сектор и обществените услуги — възможност да овладеят цифровата трансформация.

2.2. Научните изследвания в Европа откриват възможности за инвестиции за потенциални технологични пробиви и водещи инициативи, по-специално в рамките на програма „Хоризонт 2020“/„Хоризонт Европа“ и с помощта на публично-частни партньорства.

³⁵ УД: управление по дейности; БД: бюджетиране по дейности.

³⁶ Съгласно член 54, параграф 2, буква а) или б) от Финансовия регламент.

1.4.3. Очаквани резултати и отражение

Да се посочи въздействието, което предложението/инициативата следва да окаже по отношение на бенефициерите/целевите групи.

Експертният център, заедно с Мрежата и общността, ще се стреми да постигне следните цели:

- (1) да допринася за изпълнението на свързаната с киберсигурността част от програмата „Цифрова Европа“, създадена с Регламент № XXX, и по-специално дейностите, свързани с член 6 от Регламент (ЕС) № XXX [програмата „Цифрова Европа“], и от програмата „Хоризонт Европа“, създадена с Регламент № XXX, и по-специално приложение I, раздел 2.2.6 към Решение № XXX за създаване на специфичната програма за изпълнение на „Хоризонт Европа“ — рамковата програма за научни изследвания и иновации, и други програми на Съюза, когато това е предвидено в правните актове на Съюза;
- (2) да подобрява капацитета, знанията и инфраструктурата, свързани с киберсигурността, в услуга на отраслите и публичния сектор, както и научноизследователските общности;
- (3) да допринася за широкото разпространение на най-новите продукти и решения за киберсигурност в цялата икономика;
- (4) да подобрява разбирането за киберсигурността и да допринася за намаляване недостига на умения в сферата на киберсигурността в Съюза;
- (5) да допринася за укрепване на научните изследвания и развитието в сферата на киберсигурността в Съюза;
- (6) да подобрява сътрудничеството между гражданския сектор и сектора, свързан с отбраната, по отношение на технологиите и приложенията с двойна употреба;
- (7) да засилва полезните взаимодействия между гражданското и свързаното с отбраната измерение на киберсигурността;
- (8) да подпомага координирането и да улеснява работата на Мрежата от национални координационни центрове („Мрежата“), посочена в член 10, и експертната общност в сферата на киберсигурността, посочена в член 12.

1.4.4. Показатели за резултатите и за отражението

Да се посочат показателите, които позволяват да се проследи изпълнението на предложението/инициативата.

- Брой на съвместно придобитите инфраструктури и/или инструменти за киберсигурност.
- Осигурени възможности за часове на достъп до изпитвателни и експериментални инфраструктури за европейските изследователи и отрасли в цялата Мрежа и в рамките на Експертния център. В случай на вече съществуващи съоръжения, колко се увеличава броят часове на разположение за тези общности в сравнение с настоящия им брой.
- Броят на обслужваните потребителски общности и броят на изследователите, които имат достъп до европейски съоръжения за киберсигурност, се увеличава в сравнение с броя на онези, които трябва да търсят такива ресурси извън Европа.

- Наблюдава се растеж на конкурентоспособността на европейските доставчици, измерена като дял от световния пазар (целеви пазарен дял до 2027 г. — 27 %) и като дял от внедряваните в промишлеността резултати от европейската научноизследователска и развойна дейност.
- Принос към технологиите за киберсигурност от следващо поколение, измерен по отношение на авторските права, патентите, научните публикации и търговските продукти.
- Брой оценени и съгласувани учебни програми в областта на киберсигурността, брой оценени програми за професионално сертифициране в областта на киберсигурността;
- Брой обучени учени, студенти и ползватели (от промишлеността и от публичната администрация).

1.5. Мотиви за предложението/инициативата

1.5.1. Изисквания, които трябва да бъдат изпълнени в краткосрочна или дългосрочна перспектива, включително подробен график за изпълнението на инициативата

Да се постигне критична маса на инвестициите за технологични и промишлени разработки в сферата на киберсигурността и да се преодолее фрагментирането на съответния капацитет, разпръснат в ЕС.

1.5.2. Добавена стойност от намесата на ЕС

Киберсигурността е въпрос от общ интерес за Съюза, както е потвърдено в Заключенията на Съвета, посочени по-горе. Мащабът и трансграничният характер на кибератаки като WannaCry или NonPetya са важно основание за това. Естеството и мащабът на технологичните предизвикателства пред киберсигурността, а също и недостатъчната координация на усилията в рамките на промишлеността, както и между промишления и публичния сектор и научноизследователските общности, налагат на ЕС допълнително да подкрепи усилията за координиране, както за да обедини критична маса от ресурси, така и за да осигури по-добри познания и управление на активите. Това е необходимо с оглед на изискванията относно ресурсите, свързани с определени възможности за изследване, разработване и внедряване на продукти и услуги за киберсигурност; необходимостта да се предостави достъп до интердисциплинарен експертен опит в сферата на киберсигурността между различните дисциплини (каквото често съществува само отчасти на национално равнище); глобалния характер на промишлените вериги за създаване на стойност, както и дейността на конкурентите в световен мащаб, която те осъществяват на различните пазари.

Това изисква ресурси и експертни познания с мащаб, който трудно може да бъде постигнат чрез индивидуалните действия на която и да е държава членка. Така например, за общеевропейска мрежа за квантови комуникации може да са необходими инвестиции от ЕС от порядъка на 900 милиона евро, в зависимост от инвестициите от държавите членки (за свързване/допълване) и това до каква степен технологията ще позволи повторното използване на съществуващи инфраструктури.

1.5.3. *Поуки от подобен опит в миналото*

В междинната оценка на програмата „Хоризонт 2020“ наред с друго беше потвърдено, че подкрепата на ЕС за научноизследователската и развойна дейност и за справяне с обществените предизвикателства (сред които „сигурни общества“, по линия на което се подпомага научноизследователската и развойна дейност в областта на киберсигурността), продължава да бъде значима. В същото време оценката потвърждава, че укрепването на водещите позиции в промишлеността все още е предизвикателство и че продължава да има недостиг в областта на иновациите, като ЕС изостава в революционните иновации, които създават пазари.

Междинната оценка на Механизма за свързване на Европа (МСЕ) изглежда потвърждава, че добавената стойност от намесата на ЕС не се изчерпва с научноизследователската и развойна дейност, макар че киберсигурността в рамките на МСЕ има малко по-различен фокус (върху оперативната сигурност) и интервенционната логика. Същевременно по-голямата част от получателите на безвъзмездни средства за киберсигурност в рамките на МСЕ — общността на националните екипи за реагиране при инциденти с компютърната сигурност — изразиха желание за специално предназначена програма за подкрепа в рамките на следващата МФР.

Създаването през 2016 г. на публично-частно партньорство (договорно публично-частно партньорство — ДПЧП) в областта на киберсигурността в ЕС беше солидна първа стъпка, която обедини общностите от научноизследователския, промишления и публичния сектор, за да се улеснят научните изследвания и иновациите в областта на киберсигурността, и която в границите на финансовата рамка за периода 2014 — 2020 г. следва да доведе до добри, по-целенасочени резултати в областта на научните изследвания и иновациите. Договорното публично-частно партньорство позволи на партньорите от промишления сектор да поемат задължения за индивидуалните разходи, които ще направят по областите, определени в стратегическата програма за научни изследвания и иновации на ДПЧП.

1.5.4. *Съгласуваност и евентуални полезни взаимодействия с други подходящи инструменти*

Мрежата за компетентност в сферата на киберсигурността и Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността ще действат като допълнителна подкрепа на съществуващите разпоредби и участници в областта на политиката за киберсигурността. Мандатът на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността ще допълва усилията на ENISA, но има различен фокус и изисква различен набор от умения. Докато ENISA изпълнява консултативна роля при научните изследвания и иновациите в областта на киберсигурността в ЕС, предложеният мандат на центъра се съсредоточава преди всичко върху други задачи, които са от съществено значение за укрепване на устойчивостта срещу киберзаплахи в ЕС. Центърът следва да насърчава развитието и внедряването на технологии за киберсигурност и да допълва действията за изграждане на потенциал в тази област на равнището на ЕС и на национално равнище.

Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността, заедно с Мрежата за компетентност в сферата на киберсигурността, ще работят и за подпомагане на научните изследвания с цел улесняване и ускоряване на процесите по стандартизация и сертифициране, и по-специално онези, свързани със схемите за сертифициране на киберсигурността по смисъла на Акта за киберсигурността.

Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността ще играе ролята на единен механизъм за изпълнение на две европейски програми за подпомагане на киберсигурността (програмите „Цифрова Европа“ и „Хоризонт Европа“) и ще засили съгласуваността и полезните взаимодействия между тях.

Настоящата инициатива позволява да се допълнят усилията на държавите членки, като се осигури подходящ принос за създателите на политики в областта на образованието, за да се подобри образованието в областта на киберсигурността (например чрез разработване на учебни програми по въпросите на киберсигурността в гражданската и военната образователна система, но и на принос за основно образование в областта на киберсигурността). Тя ще позволи също така да се подкрепят съгласуването и непрекъснатото оценяване на програмите за професионално сертифициране в областта на киберсигурността — всички необходими дейности, които да помогнат за преодоляване на недостига на умения в сферата на киберсигурността и да улеснят достъпа на отраслите и другите общности до специалисти по киберсигурност. Съгласуването на образованието и уменията ще подпомогне развитието на квалифицирана в областта на киберсигурността работна сила в ЕС — ключов актив за предприятията в сектора на киберсигурността, както и за други отрасли с интереси в областта на киберсигурността.

1.6. Срок на действие и финансово отражение

☒ Предложение/инициатива с **ограничен срок на действие**

- ☒ Предложението/инициативата е в сила от 1.1.2021 г. до 31.12.2029 г.
- ☒ Финансово отражение от 2021 г. до 2027 г. за бюджетните кредити за поети задължения и от 2021 г. до 2031 г. за бюджетните кредити за плащания.
- ☐ Предложение/инициатива с **неограничен срок на действие**
 - Изпълнение с период на започване на дейност от ГТТГ до ГТТГ,
 - последван от функциониране с пълен капацитет.

1.7. Планирани методи на управление³⁷

☐ **Пряко управление** от Комисията

- ☐ от нейните служби, включително от нейния персонал в делегациите на Съюза;
- ☐ от изпълнителните агенции

☐ **Споделено управление** с държавите членки

☒

Непряко управление чрез възлагане на задачи по изпълнението на бюджета на:

- ☐ трети държави или на органите, определени от тях;
- ☐ международни организации и техните агенции (да се уточни);
- ☐ ЕИБ и Европейския инвестиционен фонд;
- ☒ органите, посочени в членове 70 и 71 от Финансовия регламент;
- ☐ публичноправни органи;
- ☐ частноправни органи със задължение за обществена услуга, доколкото предоставят подходящи финансови гаранции;
- ☐ органи, уредени в частното право на държава членка, на които е възложено осъществяването на публично-частно партньорство и които предоставят подходящи финансови гаранции;
- ☐ лица, на които е възложено изпълнението на специфични дейности в областта на ОВППС съгласно дял V от ДЕС и които са посочени в съответния основен акт.
- *Ако е посочен повече от един метод на управление, пояснете в частта „Забележки“.*

³⁷

Подробности във връзка с методите на управление и позоваванията на Финансовия регламент могат да бъдат намерени на уебсайта BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_bg.html

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

Да се посочат честотата и условията.

Член 28 съдържа подробни разпоредби относно мониторинга и докладването.

2.2. Система за управление и контрол

2.2.1. Установени рискове

За да се намалят рисковете, свързани с функционирането на Експертния център след неговото създаване, както и евентуалните закъснения, Комисията ще подкрепя Експертния център през тази фаза, за да осигури бързото наемане на ключов персонал и изграждането на ефикасна система и ясни процедури за вътрешен контрол.

2.2.2. Информация за структурата на системата за вътрешен контрол

Изпълнителният директор отговаря за дейността и ежедневното управление на Експертния център и е неговият законен представител. Директорът отговаря пред управителния съвет и периодично му докладва за развитието на дейността на Експертния център.

Управителният съвет носи цялата отговорност за стратегическата ориентация и функционирането на Експертния център и следи за изпълнението на неговите дейности.

Финансовите правила, приложими за Експертния център, се приемат от управителния съвет след консултация с Комисията. Те не се отклоняват от Регламент (ЕС) № 1271/2013, освен ако специфичните изисквания за функционирането на Експертния център го налагат и ако Комисията е дала предварителното си съгласие.

Вътрешният одитор на Комисията упражнява същите правомощия по отношение на Експертния център, каквито упражнява по отношение на Комисията. Сметната палата има правомощия за извършване на одити по документи и на място на всички бенефициери на безвъзмездни средства, изпълнители и подизпълнители, които са получили средства от Съюза чрез Експертния център.

2.2.3. Оценка на разходите и ползите от проверките и на очакваната степен на риск от грешка

Разходи за проверките и ползи от тях

Разходите за проверки за Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността се разделят на разходи за надзор на равнището на Комисията и разходи за оперативни проверки на равнището на изпълнителния орган.

Разходите за проверки на равнището на Експертния център се оценяват на около 1,19 % от бюджетните кредити за оперативни плащания, усвоени на равнището на Експертния център.

Разходите за надзор на равнището на Комисията се оценяват на около 1,20 % от бюджетните кредити за оперативни плащания, усвоени на равнището на Експертния център.

При допускането, че дейностите ще се управляват изцяло от Комисията без подкрепата на изпълнителния орган, разходите за проверки биха били значително по-високи и биха могли да достигнат около 7,7 % от бюджетните кредити за плащания.

Предвидените проверки имат за цел да гарантират плавен и ефективен надзор на изпълнителните органи от страна на Комисията и да осигурят необходимата степен на увереност на равнището на Комисията.

Ползите от проверките са следните:

- предотвратяване на избора на по-слаби или несъответстващи предложения;
- оптимизиране на планирането и използването на средства от ЕС, така че да се запази добавената стойност от ЕС;
- гарантиране на качеството на споразуменията за отпускане на безвъзмездни средства, като се избягват грешки в идентификацията на правните субекти, осигурява се правилното изчисляване на вноските от ЕС и се получават необходимите гаранции за правилното използване на отпуснатите безвъзмездни средства;
- откриване на недопустими разходи на етапа на плащането;
- откриване на грешки във връзка със законосъобразността и редовността на операциите на етапа на контрола.

Изчислен процент грешки

Целта е процентът на остатъчна грешка да се задържи под прага от 2 % за цялата програма, като същевременно се ограничи тежестта на контрола за бенефициерите, за да се постигне правилният баланс между целта за законосъобразност и редовност и другите цели, като например привлекателността на програмата, особено за малките и средните предприятия, и разходите за проверките.

2.3. Мерки за предотвратяване на измами и нередности

Да се посочат съществуващите или планираните мерки за превенция и защита.

OLAF може да извършва разследвания, включително проверки и инспекции на място, в съответствие с разпоредбите и процедурите, предвидени в Регламент (ЕС, Евратом) № 883/2013 на Европейския парламент и на Съвета и Регламент (Евратом, ЕО) № 2185/9640 на Съвета от 11 ноември 1996 г. относно контрола и проверките на място, извършвани от Комисията за защита на финансовите интереси на Европейския съюз срещу измами и други нередности, с цел да се установи дали е налице измама, корупция или друга незаконна

дейност, накърняваща финансовите интереси на Съюза, във връзка с безвъзмездни средства или поръчка, финансирани от Експертния център.

Споразуменията, решенията и договорите, произтичащи от прилагането на настоящия регламент, съдържат разпоредби, които изрично упълномощават Комисията, Експертния център, Сметната палата и OLAF да извършват одити и разследвания съгласно предоставените им съответни правомощия.

Експертният център гарантира, че финансовите интереси на неговите членове са защитени по подходящ начин, като осъществява или възлага на други осъществяването на подходящ вътрешен и външен контрол.

Експертният център се присъединява към Междуйнституционалното споразумение от 25 май 1999 г. между Европейския парламент, Съвета на Европейския съюз и Комисията на Европейските общности относно вътрешните разследвания, провеждани от Европейската служба за борба с измамите (OLAF). Експертният център приема необходимите мерки за улесняване на вътрешните разследвания, извършвани от OLAF.

Експертният център ще приеме стратегия за борба с измамите въз основа на анализ на рисковете от измами и на съображения относно на разходите и ползите. Той защитава финансовите интереси на Съюза чрез прилагането на превантивни мерки срещу измами, корупция и всякакви други незаконни дейности посредством ефективни проверки и, при наличие на нередности, чрез събирането на недължимо платените суми, а също така, когато това е целесъобразно, чрез ефективни, съразмерни и възпиращи административни и финансови санкции.

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

3.1. Функция от многогодишната финансова рамка и предложени нови разходни бюджетни редове

- Поискани нови бюджетни редове

По реда на функциите от многогодишната финансова рамка и на бюджетните редове:

Функция от многогодишната финансова рамка	Бюджетен ред	Вид на разхода	Вноска			
	Номер	Многогод./едногод. ³⁸	от държави от ЕАСТ ³⁹	от държави кандидатки ⁴⁰	от трети държави	по смисъла на член [21, параграф 2, буква б)] от Финансовия регламент
Функция I : Единен пазар, иновации и цифрови технологии	01 02 XX XX Център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността по „Хоризонт Европа“ — разходи за подкрепа	Многого д.	ДА	ДА (ако е посочен в годишната работна програма)	ДА (ограничен до някаква част от програмата)	НЕ
	01 02 XX XX Център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността по „Хоризонт Европа“					
	02 06 01 XX Център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността по програма „Цифрова Европа“ — разходи за подкрепа					
	02 06 01 XX Център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността по					

³⁸ Многогод. = многогодишни бюджетни кредити / едногод. = едногодишни бюджетни кредити.

³⁹ ЕАСТ: Европейска асоциация за свободна търговия.

⁴⁰ Държави кандидатки и, ако е приложимо, потенциални кандидатки от Западните Балкани.

	програма „Цифрова Европа“					
--	---------------------------	--	--	--	--	--

- Вноските по този бюджетен ред се очаква да постъпят от:

млн. евро (до 3-тия знак след десетичната запетая)

Бюджетен ред	Година 2021	Година 2022	Година 2023	Година 2024	Година 2025	Година 2026	Година 2027	Общо
01 01 01 01 Разходи, свързани с длъжностни лица и временно наети лица, изпълняващи научни изследвания — „Хоризонт Европа“	р.м.	р.м.	р.м.	р.м.	р.м.	р.м.	р.м.	р.м.
01 01 01 02 Външен персонал, изпълняващ програми за научни изследвания — „Хоризонт Европа“	р.м.	р.м.	р.м.	р.м.	р.м.	р.м.	р.м.	р.м.
01 01 01 03 Други разходи за управление във връзка с научни изследвания — „Хоризонт Европа“	р.м.	р.м.	р.м.	р.м.	р.м.	р.м.	р.м.	р.м.
01 02 02 Глобални предизвикателства и конкурентоспособност на промишлеността	р.м.	р.м.	р.м.	р.м.	р.м.	р.м.	р.м.	р.м.
02 01 04 Административна подкрепа — програма „Цифрова Европа“	1 238	3 030	3 743	3 818	3 894	3 972	4 051	23 746
02 06 01 Киберсигурност — програма „Цифрова Европа“	284 892	322 244	327 578	248 382	253 295	258 214	263 316	1 957 922
Общо разходи	286 130	325 274	331 320	252 200	257 189	262 186	267 368	1 981 668

Финансовата вноска от финансовия пакет на клъстера „Приобщаващо и сигурно общество“ по стълб II „Глобални предизвикателства и конкурентоспособност на промишлеността“ от програма „Хоризонт Европа“ (общ пакет на стойност 2 800 000 000 евро), посочена в член 21, параграф 1, буква б), ще бъде предложена от Комисията по време на законодателния

процес и във всеки случай преди да бъде постигнато политическо споразумение. Предложението ще се основава на резултатите от процеса на стратегическо планиране, както е определено в член 6, параграф 6 от Регламент XXX [рамкова програма „Хоризонт Европа“].

Горните суми не включват вноската от държавите членки за покриване на оперативните и административните разходи на Експертния център, съизмерима с финансовата вношка от Съюза.

3.2. Очаквано отражение върху разходите

3.2.1. Обобщение на очакваното отражение върху разходите

млн. евро (до 3-тия знак след десетичната запетая)

Функция от многогодишната финансова рамка	1	Единен пазар, иновации и цифрова икономика
--	----------	--

			2021 г. 41	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	След 2027 г.	ОБЩО
Дял 1 (разходи за персонал)	Поети задължения = Плащания	(1)	619	1 515	1 871	1 909	1 947	1 986	2 026		11 873
Дял 2 (Разходи за инфраструктура и оперативни разходи)	Поети задължения = Плащания	(2)	619	1 515	1 871	1 909	1 947	1 986	2 026		11 873
Дял 3 (оперативни разходи)	Поети задължения	(3)	284 892	322 244	327 578	248 382	253 295	258 214	263 316		1 957 922
	Плащания	(4)	21 221	102 765	150 212	167 336	156 475	150 124	148 074	1 061 715	1 957 922
ОБЩО бюджетни кредити за	Поети задължения	= 1+2+3	286 130	325 274	331 320	252 200	257 189	262 186	267 368		1 981 668

⁴¹ Бюджетните кредити за персонал за 2021 г. са отчетени само за шест месеца.

финансовия пакет на програмите⁴²	Плащания	= 1+2+4	22 459	105 795	153 954	171 154	160 369	154 096	152 126	1 061 715	1 981 668
--	----------	------------	--------	---------	---------	---------	---------	---------	---------	-----------	-----------

⁴² Посоченият общ размер на бюджетните кредити се отнася само за финансови ресурси от ЕС, предназначени за киберсигурност в рамките на програма „Цифрова Европа“. Финансовата вноска от финансовия пакет на клъстера „Приобщаващо и сигурно общество“ по стълб II „Глобални предизвикателства и конкурентоспособност на промишлеността“ от програма „Хоризонт Европа“ (общ пакет на стойност 2 800 000 000 евро), посочена в член 5, параграф 1, буква б), ще бъде предложена от Комисията по време на законодателния процес и във всеки случай преди да бъде постигнато политическо споразумение. Предложението ще се основава на резултатите от процеса на стратегическо планиране, както е определено в член 6, параграф 6 от Регламент XXX [рамкова програма „Хоризонт Европа“].

Функция от многогодишната финансова рамка	7	„Административни разходи“
--	----------	---------------------------

млн. евро (до 3-тия знак след десетичната запетая)

		2021 г.	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	След 2027 г.	ОБЩО
Човешки ресурси		3 090	3 233	3 233	3 233	3 233	3 233	3 805		23 060
Други административни разходи		105	100	104	141	147	153	159		909
ОБЩО бюджетни кредити по ФУНКЦИЯ 7 от многогодишната финансова рамка	(Общо задължения = поети плащания)	3 195	3 333	3 337	3 374	3 380	3 386	3 964		23 969

млн. евро (до 3-тия знак след десетичната запетая)

		2021 г.	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	След 2027 г.	ОБЩО
ОБЩО бюджетни кредити по всички ФУНКЦИИ от многогодишната финансова рамка	Поети задължения	289 325	328 607	334 657	255 574	260 569	265 572	271 332		2 005 637
	Плащания	25 654	109 128	157 291	174 528	163 749	157 482	156 090	1 061 715	2 005 637

3.2.2. Резюме на очаквано отражение върху бюджетните кредити за административни разходи

- ☐ Предложението/инициативата не налага използване на бюджетни кредити за административни разходи
- ☒ Предложението/инициативата налага използване на бюджетни кредити за административни разходи съгласно обяснението по-долу:

млн. евро (до 3-тия знак след десетичната запетая)

Години	2021 г.	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	ОБЩО
--------	---------	---------	---------	---------	---------	---------	---------	------

ФУНКЦИЯ 7 от многогодишната финансова рамка								
Човешки ресурси	3 090	3 233	3 233	3 233	3 233	3 233	3 805	23 060
Други административни разходи	105	100	104	141	147	153	159	909
Междинен сбор по ФУНКЦИЯ 7 от многогодишната финансова рамка	3 195	3 333	3 337	3 374	3 380	3 386	3 964	23 969

Извън ФУНКЦИЯ 7⁴³ от многогодишната финансова рамка								
Човешки ресурси								
Други разходи от административно естество	1 238	3 030	3 743	3 818	3 894	3 972	4 051	23 746
Междинен сбор извън ФУНКЦИЯ 7 от многогодишната финансова рамка	1 238	3 030	3 743	3 818	3 894	3 972	4 051	23 746

ОБЩО	4 433	6 363	7 079	7 192	7 274	7 358	8 016	47 715
-------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	---------------

Бюджетните кредити, необходими за човешки ресурси и други разходи от административно естество, ще бъдат покрити от бюджетни кредити на ГД, които вече са определени за управлението на действието и/или които са преразпределени в рамките на ГД, при необходимост заедно с допълнително отпуснати ресурси, които могат да бъдат предоставени на управляващата ГД в рамките на годишната процедура за отпускане на средства и като се имат предвид бюджетните ограничения.

Посочените по-горе бюджетни кредити, необходими за човешки ресурси и други разходи от административно естество, попадащи извън функция 7, съответстват на сумите, покрити от финансовата вноска на Съюза от програма „Цифрова Европа“.

⁴³ Техническа и/или административна помощ и разходи в подкрепа на изпълнението на програми и/или дейности на ЕС (предишни редове ВА), непреки научни изследвания, преки научни изследвания.

Бюджетните кредити, необходими за човешки ресурси и други разходи от административно естество, попадащи извън функция 7, ще бъдат увеличени със сумите, които се покриват от финансовата вноска на Съюза от програма „Хоризонт Европа“, след като финансовата вноска от финансовия пакет на клъстера „Приобщаващо и сигурно общество“ по стълб II „Глобални предизвикателства и конкурентоспособност на промишлеността“ по програма „Хоризонт Европа“ (общ пакет на стойност 2 800 000 000 евро), посочена в член 21, параграф 1, буква б), бъде предложена от Комисията по време на законодателния процес, но във всеки случай преди да бъде постигнато политическо споразумение.

Посочените по-горе суми на бюджетните кредити, необходими за човешки ресурси и други разходи от административно естество, попадащи извън функция 7, не включват вноската от държавите членки за покриване на административните разходи на Експертния център, съизмерима с финансовата вноска от Съюза.

3.2.2.1. Очаквани нужди от човешки ресурси в Комисията

- ☐ Предложението/инициативата не налага използване на човешки ресурси
- ☒ Предложението/инициативата налага използване на човешки ресурси съгласно обяснението по-долу:

Оценката се посочва в еквиваленти на пълно работно време

Години		2021 г.	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.
• Длъжности в щатното разписание (длъжностни лица и временно наети служители)								
Централа и представителства на Комисията		20	21	21	21	21	21	22
Делегации								
Научни изследвания								
• Външен персонал (в еквивалент на пълно работно време — ЕПРВ) — ДНП, МП, КНЕ, ПНА, МЕД ⁴⁴								
Функция 7								
Финансирани от ФУНКЦИЯ 7 от многогодишната финансова рамка	- в централата	3	3	3	3	3	3	3
	- в делегациите							
Финансирани от финансовия пакет на програмата ⁴⁵	- в централата							
	- в делегациите							
Научни изследвания								
Други бюджетни редове (да се посочат)								
ОБЩО		23	23	24	24	24	25	25

Нуждите от човешки ресурси ще бъдат покрити от персонала на ГД, на който вече е възложено управлението на дейността и/или който е преразпределен в рамките на ГД, при необходимост заедно с всички допълнителни отпуснати ресурси, които могат да бъдат предоставени на управляващата ГД в рамките на годишната процедура за отпускане на средства и като се имат предвид бюджетните ограничения.

Описание на задачите, които трябва да се изпълняват:

Длъжностни лица и временно наети служители	Координиране, мониторинг и управление на задачите, възложени на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността, включително разходи за подкрепа и координиране. Разработване и координиране на политика в областта на киберсигурността по отношение на задачите, възложени на Европейския център за промишлени, технологични и изследователски експертни познания в областта на
--	--

⁴⁴ ДНП = договорно нает персонал; МП = местен персонал; КНЕ = командирован национален експерт; ПНА = персонал, нает чрез агенции за временна заетост; МЕД = младши експерт в делегация.

⁴⁵ Подтаван за външния персонал, покрит с бюджетните кредити за оперативни разходи (предишни редове ВА).

	киберсигурността, например във връзка с определянето на приоритети за политиката в областта на научните изследвания и промишлеността, общото сътрудничество между държавите членки и икономическите оператори, съгласуваността с бъдещата рамка на ЕС за сертифициране за киберсигурност, работата по въпросите на отговорността и задълженията за полагане на дължима грижа или координацията с политиките в областта на високопроизводителните изчислителни технологии, изкуствения интелект и цифровите умения. .
Външен персонал	Координиране, мониторинг и управление на задачите, възложени на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността, включително разходи за подкрепа и координиране. Разработване и координиране на политика в областта на киберсигурността по отношение на задачите, възложени на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността, например във връзка с определянето на приоритети за политиката в областта на научните изследвания и промишлеността, общото сътрудничество между държавите членки и икономическите оператори, съгласуваността с бъдещата рамка на ЕС за сертифициране за киберсигурност, работата по въпросите на отговорността и задълженията за полагане на дължима грижа или координацията с политиките в областта на високопроизводителните изчислителни технологии, изкуствения интелект и цифровите умения. .

3.2.2.2. Очаквани нужди от човешки ресурси на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността

	2021 г.	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.
Длъжностни лица от Комисията							
от които AD							
от които AST							
от които AST-SC							
Временно наети лица							
от които AD	10	11	13	13	13	13	13
от които AST							
от които AST-SC							
Договорно наети служители	26	32	39	39	39	39	39
КНЕ	1	1	1	1	1	1	1
Общо	37	44	53	53	53	53	53

Описание на задачите, които трябва да се изпълняват:

Длъжностни лица и временно наети служители	Оперативно изпълнение на задачите, възложени на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността съгласно член 4 от настоящия регламент, включително разходи за подкрепа и координиране.
Външен персонал	Оперативно изпълнение на задачите, възложени на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността съгласно член 4 от настоящия регламент, включително разходи за подкрепа и координиране.

Посочените по-горе очаквани нужди от човешки ресурси на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността съответстват на очакваните нужди за изпълнение на финансовата вноска от Съюза по програма „Цифрова Европа“.

Посочените по-горе очаквани нужди от човешки ресурси на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността ще бъдат увеличени с очакваните нужди за изпълнение на финансовата вноска от Съюза по програма „Хоризонт Европа“, след като вноската от финансовия пакет на клъстера „Приобщаващо и сигурно общество“ по стълб II „Глобални предизвикателства и конкурентоспособност на промишлеността“ по програма „Хоризонт Европа“ (общ пакет на стойност 2 800 000 000 евро), посочена в член 21, параграф 1, буква б), бъде предложена от Комисията по време на законодателния процес, но във всеки случай преди да бъде постигнато политическо споразумение.

3.2.2.3. Щатно разписание на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността

Функционална група и степен	2021 г.	2022 г.	2023 г.	2024 г.	2025 г.	2025 г.	2025 г.
AD 16							
AD 15							
AD 14	1	1	1	1	1	1	1
AD 13							
AD 12							
AD 11							
AD 10							
AD 9	5	5	6	6	6	6	6
AD 8	1	1	1	1	1	1	1
AD 7	1	2	3	3	3	3	3
AD 6	1	1	1	1	1	1	1
AD 5	1	1	1	1	1	1	1
Общо AD	10	11	13	13	13	13	13
AST 11							
AST 10							
AST 9							
AST 8							
AST 7							
AST 6							
AST 5							

AST 4							
AST 3							
AST 2							
AST 1							
Общо AST							
AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							
AST/SC 2							
AST/SC 1							
Общо AST/SC							
ОБЩО ВСИЧКО	10	11	13	13	13	13	13

3.2.2.4. Очаквано отражение върху персонала (допълнителни ЕПРВ) — външен персонал на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността

Договорно наети служители	2021 г.	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.
Функционална група IV	20	22	29	29	29	29	29
Функционална група III	2	4	4	4	4	4	4
Функционална група II	4	6	6	6	6	6	6
Функционална група I							
Общо	26	32	39	39	39	39	39

За да се гарантира неутралност на числеността, допълнителните бройки персонал в Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността отчасти ще се компенсират чрез намаляване на броя длъжностни лица и външен персонал (т.е. от действащото щатно разписание и плана за външния персонал) в съответните служби на Комисията.

Бройките на персонала на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността в точки 3.2.2.2 — 4 ще бъдат компенсирани, както следва⁴⁶:

ОБЩО	2021 г.	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.
Длъжностни лица от Комисията	5	5	6	6	6	6	6
Временно наети лица							
Договорно наети служители	14	17	20	20	20	20	20
КНЕ							
Общо ЕПРВ	19	22	26	26	26	26	26
Численост	19	22	26	26	26	26	26

Компенсирането на човешките ресурси в Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността ще бъде съизмеримо с дела на финансовата вноска на Съюза, т.е. 50 %.

Посоченото по-горе компенсиране се отнася за очакваните нужди от човешки ресурси на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността за изпълнение на финансовата вноска от Съюза по програма „Цифрова Европа“.

Посоченото по-горе компенсиране ще бъде увеличено с очакваните нужди за изпълнение на финансовата вноска на Съюза от програма „Хоризонт Европа“, след като вноската от финансовия пакет на клъстера „Приобщаващо и сигурно общество“ по стълб II „Глобални предизвикателства и конкурентоспособност на промишлеността“ по програма „Хоризонт Европа“ (общ пакет на стойност 2 800 000 000 евро), посочена в член 21, параграф 1, буква б), бъде предложена от Комисията по време на законодателния процес, но във всеки случай преди да бъде постигнато политическо споразумение.

⁴⁶ В зависимост от окончателния размер на бюджета, чието изпълнение ще бъде делегирано на Експертния център

3.2.3. Финансов принос от трети страни

Предложението/инициативата:

- ☐ не предвижда съфинансиране от трети страни
- ☒ предвижда следното съфинансиране от трети страни⁴⁷, като оценките са дадени по-долу:

Бюджетни кредити в млн. евро (до 3-тия знак след десетичната запетая)

Години	2021 г.	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	ОБЩО
Държави членки — вноски за покриване на разходи за персонал	619	1 515	1 871	1 909	1 947	1 986	2 026	11 873
Държави членки — вноски за покриване на разходи за инфраструктура и оперативни разходи	619	1 515	1 871	1 909	1 947	1 986	2 026	11 873
Държави членки — вноски за покриване на оперативни разходи	284 892	322 244	327 578	248 382	253 295	258 214	263 316	1 957 922
ОБЩО съфинансирани бюджетни кредити	286 130	325 274	331 320	252 200	257 189	262 186	267 368	1 981 668

Посоченият по-горе финансов принос от трети страни се отнася само за съфинансирането, съизмеримо с финансовите ресурси от ЕС, предназначени за киберсигурност в рамките на програма „Цифрова Европа“. Посоченият по-горе финансов принос от трети страни ще бъде увеличен, след като финансовата вноска от клъстера „Приобщаващо и сигурно общество“ по стълб II „Глобални предизвикателства и конкурентоспособност на промишлеността“ от програма „Хоризонт Европа“ (общ пакет на стойност 2 800 000 000 евро), посочена в член 21, параграф 1, буква б), ще бъде предложена от Комисията по време на законодателния процес и във всеки случай преди да бъде постигнато политическо споразумение. Предложението ще се основава на резултатите от процеса на стратегическо планиране, както е определено в член 6, параграф 6 от Регламент XXX [рамкова програма „Хоризонт Европа“].

3.3. Очаквано отражение върху приходите

- ☒ Предложението/инициативата няма финансово отражение върху приходите
- ☐ Предложението/инициативата има следното финансово отражение:
 - ☐ върху собствените ресурси
 - ☐ върху разните приходи

Моля, посочете дали приходите са записани по разходни бюджетни редове. ☐

млн. евро (до 3-тия знак след десетичната запетая)

⁴⁷ Очаквана непарична вноска от държавите членки

Приходен ред:	отражение на предложението/инициативата ⁴⁸						
	2021 г.	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.
Статия							

За целевите приходи да се посочат съответните разходни бюджетни редове.

Други забележки (например метод/формула за изчисляване на отражението върху приходите или друга информация).

⁴⁸

Що се отнася до традиционните собствени ресурси (мита, налози върху захарта), посочените суми трябва да бъдат нетни, т.е. брутни суми, от които са приспаднати 20 % за разходи по събирането.